PUBLIC SUBMISSION

As of: 3/28/22 9:50 AM
Received: March 24, 2022
Status: Pending_Post
Tracking No. l15-edfx-z1z5
Comments Due: April 25, 2022
Submission Type: Web

Docket: NIST-2022-0001
Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

Comment On: NIST-2022-0001-0001
RFI-2022-03642

Document: NIST-2022-0001-DRAFT-0016
Comment on FR Doc # N/A

Submitter Information

Name: Daniel Sela
Address:
New York, NY, 10009

General Comment

I would like to see data governance and security guidelines for data shared or stored by vendors.
I would like to see more guidelines to form best practices around how to limit the storage of sensitive data with external vendors.

an example using the recent Okta breach is that many companies use Okta as an authentication and authorization provider, but it is not necessary to store sensitive customer data in Okta to get these benefits from the service.
e.g.
- the username doesn't have to be the user's email
- upon login to a system the system could translate the user's email input to an anonymized unique identified
- the anonymized unique ID can then be used to verify the user's authentication and authorization with Okta

end goal: minimize the organization's exposure to 3rd party security breaches in first place