PUBLIC SUBMISSION

As of: 4/25/22 12:30 PM
Received: April 21, 2022
Status: Pending_Post
Tracking No. l28-serr-jgnu
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-0024
Comment on FR Doc # N/A

Submitter Information

Email: [redacted]
Organization: Information Age Ltd.

General Comment

DMARC and SPF / DKIM use should be included in the standard. This enables the recipient to validate the source. Email services should report to anomalies to the forensic (ruf) address specified.

PUBLIC SUBMISSION

As of: 4/25/22 12:32 PM
Received: April 21, 2022
Status: Pending_Post
Tracking No. l28-tlpd-vg9l
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-0025
Comment on FR Doc # N/A

Submitter Information

Email: [redacted]
Organization: Information Age Ltd.

General Comment

Testing or checking for compliance with sound security practices is not achievable for many individuals, charities and other small organisations. They are, as a result open to exploitation. Can the framework include the concept of model architectures, for end user devices and for services so that these organisations can acquire a device or purchase a services that they know would be reasonable safe. For end user devices a model architecture would effectively be a device built using a public, assured "Gold Build". It may be something that Organisations such as CIS and OWASP could then publish or the vendors, Microsoft, Apple, Google could provide?