PUBLIC SUBMISSION

As of: 3/14/22 6:22 PM
Received: March 14, 2022
Status: Pending_Post
Tracking No. l0q-typ6-mnaw
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-0006
Comment on FR Doc # N/A

Submitter Information

Name: David Carpenter
Address:
Davenport, IA, 52807

General Comment

The NIST CSF is rightfully targets helping organizations both private and public to help secure their infrastructure from compromise. From a government perspective, this is where the most amount of damage is likely to occur. However, the number of devices that are part of home networks is increasing and these numbers will continue to rise as companies add more IoT devices to the ecosystem. Recently my plumber offered to install a WiFi enabled sump pump. The majority of people that are installing new IoT, to include this plumber, are not cybersecurity experts and they leave securing IoT items to the homeowner. Most people assume that they are best with the factory settings, to include the default admin and password. All of these devices to include home computer systems offer a large pool for potential botnets and launch points that adversaries can take advantage of in attacks against US critical infrastructure. This type of obfuscation further complicates any response to mitigate these attacks. CISA's Security Tip 15-002 (https://www.cisa.gov/uscert/ncas/tips/ST15-002) has many of the things that are worth doing but could be bolstered by having the NIST's CSF's concise design to back it up and using the NIST CSF as a guide it could help home owners to secure their networks by going beyond just these basics.