



National Institute for Standards and Technology (NIST)

June 13, 2016

Thank you for your dedication to the important issue of cybersecurity for national critical infrastructure.

Taproot Security is a private firm advising clients and policymakers on vital cybersecurity matters. We read with interest NIST's recent announcement regarding cyber security framework refinements planned for 2017. Three suggestions for your consideration:

1. We're pleased authentication will be an area of focus for the upcoming framework revision. Since special publication SP 800-63 is currently undergoing revision, I suggest coordinating efforts within NIST between the cyber framework and 800-63-3 teams to ensure alignment. Although its original audience was federal agencies, SP 800-63 has become influential among private sector critical infrastructure operators. For example, the financial services industry authentication standard [X9.117](#) is based on the 800-63 4-tier framework.
2. Taproot Security provided detailed comments on SP 800-63-3 through the [NIST GitHub](#) repository. GitHub might prove a useful way for the NIST cybersecurity framework team to interact with stakeholders with greater transparency and agility.
3. We encourage NIST to collaborate with sector specific regulatory agencies that currently oversee IT security of critical infrastructure operators. A good example is the [FFIEC](#). Their IT Examiner Handbooks constitute a cyber framework that predates NIST's work, so the two must be harmonized in order to avoid overly burdening (or possibly giving conflicting guidance to) the financial services sector.

Thank you for this opportunity to share our perspective on future direction of the NIST cybersecurity framework.

Sincerely,

A handwritten signature in black ink that reads "Michael McCormick". The signature is written over a light gray horizontal line.

Michael McCormick
President, Taproot Security
www.taprootsecurity.com
mike@taprootsecurity.com