From: Mark Formanek
Sent: Friday, January 19, 2018 11:14 AM
To: cyberframework <cyberframework@nist.gov>
Subject: NIST Cyber Security Framework and Roadmap Comments

To whom it may concern,
On behalf of Spry Methods I have attached the comments for Cyber Security Framework and Roadmap.
Thank you,
Mark Formanek

Mark Formanek, CISSP
Cyber Security Lead

Spry Methods
1420 Spring Hill Road Suite 300 | McLean, Virginia, 22102
o: 703.600.7779 | f: 703.600.7799 | e: info@sprymethods.com

[***Attachment copied below***]

CYBERSECURITY FRAMEWORK 1.1 COMMENTS

Page	Line Number	Change / Update
E.g. (P. 13)	***(429-430)***	***(Remove "and an organization-wide approach to managing cybersecurity risk has not been established")***
P. 9	Line 206	"support" should be "supports"
P. 11	Line 297	NIST is previously defined on line 96
p. 14	Line 328/329	Same diagram with two styles?
		No Framework Tiers appendix? Examples, details, etc.
		No Framework Profiles appendix? Examples, details, etc.
		Mentioning proactive defense, Offensive Countermeasures and Cyber Deception that can aid to detect, analyze, and defend against zero-day and advanced attacks, often in real time.

CYBERSECURITY ROADMAP COMMENTS

Page	Change / Update
4	***4.2 Cyber-Attack Lifecycle should include the proactive defense, Offensive Countermeasures and Cyber Deception that can aid to detect, analyze, and defend against zero-day and advanced attacks.*** ***The Department of Defense and other industry organizations realize that the best action is a pre-emptive and proactive defense to cyber security. Proactive defense is the anticipation of an attack involving software, computers, and networks. Leveraging proactive defense technology and practices aids to reduce or mitigate operational risk.*** ***Offensive Countermeasures employs unique methods of both tracking back an attacker and detecting attackers within your network. Organizations can develop a security strategy that creates consequences for the attackers who hack our computers. Countermeasures can also include negotiation, psychological warfare, cyberwarfare, economic warfare, information warfare and prosecution.*** ***Cyber Deception conceals your networks, create uncertainty and confusion against the attacker's efforts to establish situational awareness, and to influence and misdirect attacker perceptions and decision processes. Deception can belveraged as honeytokens, honeypots, and breadcrumbs.***