From: BOARDMAN, ELIZABETH
Sent: Tuesday, January 2, 2018 4:20 PM
To: cyberframework <cyberframework@nist.gov>
Subject: Comment about Cybersecurity Framework V 1.1

The cybersecurity framework core refers to the five high level function of "Identify, Protect, Detect, Respond, Recover".

Lines 378-382 - The "Respond" function refers to "Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. incident." The Respond Function supports the ability to contain the impact of a potential cybersecurity event incident. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

There is no place in the definition of "respond" or anywhere else in the document where it refers to prosecution. I believe this is sixth high level function that should be addressed. Although it may be impossible to definitely identify perpetrators in some instances, if the policies and procedures are not in place before an attack to preserve evidence, any evidence collected after the fact may not be admissible in a court of law (local, national or international).

The policies, procedures, etc. for prosecution should be included as part of "Respond" or be a sixth function of the framework.

Elizabeth Boardman