Re: Comments of Motorola Solutions Inc. to the National Institute of Standards and Technology on the Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. Draft 2 (Docket No. 130208119-3119-01)

Motorola Solutions appreciates the opportunity to offer comments on the "Cybersecurity Framework 1.1-Draft 2", which was published on December 5, 2017.

Motorola Solutions is the leading provider of mission-critical communications equipment and public safety technology. Motorola Solutions serves more than 100,000 public safety and commercial customers in more than 100 countries. Founded in 1928, Motorola has a history of innovation that has revolutionized communications. From pioneering mobile communications in the 1930s and making equipment that carried the first words from the moon in 1969, to supporting modern-day emergency response equipment for disaster relief efforts around the world.

Motorola Solutions commends the National Institute of Standards and Technology's (NIST) continued commitment to the Cybersecurity Framework (CSF). The latest CSF 1.1 Draft 2 makes thoughtful additions to the original CSF by included current industry references and expansion into emerging and developing areas related to cybersecurity. Many of the additions in the CSF 1.1 Draft 2 are already industry best practices and it is encouraging to see the CSF on parity with industry. Specifically, Motorola Solutions commends the addition in the CSF 1.1 Draft 2 of the Internet of Things (IoT), Supply Chain Risk Management (SCRM), and authentication methods. These areas represent current industry best practices and will help the CSF continue to be a viable voluntary, industry driven, self-assessment tool. The CSF must continue to follow the voluntary, industry driven, self-assessment model to remain a useful tool for the private sector. The CSF must remain flexible enough to be used across sectors and among private entities of various sizes with different risk profiles and tolerances.

I. Internet of Things (IoT)

The Internet of Things (IoT) is maturing at a rapid rate and the full impact has not been fully realized. It is clear that more and more devices, both consumer and commercial, will continue to come online in the future. All of these new IoT enabled devices represent new cybersecurity vulnerabilities that could potentially be exploited. The CSF 1.1 Draft 2 has proactively identified the risk posed to IoT and has taken the necessary steps to try and ensure the private sector has the necessary guidance on how to mitigate IoT cybersecurity threats.

II. Supply Chain Risk Management (SCRM)

Supply Chain Risk Management (SCRM) is an area of justified concerns for the private sector. In an ever evolving supply chain marketplace, the need to have accountability for components and vendors is paramount to cybersecurity. The best cybersecurity mitigation strategies are vulnerable without adequate SCRM. The CSF 1.1 Draft 2 has identified the potential risk posed by SCRM and the need to secure supply chains.

III. Authentication

The CSF 1.1 Draft 2 approaches authentication in the same manner as the private sector. Much like the private sector, the CSF 1.1 Draft 2 does not prescribe a one size fits all approach. Instead, the CSF 1.1 Draft 2 allows private sector entities to choose their own authentication requirements based on user and customer security requirements. This flexibility is paramount to ensure an entity is deploying the best authentication methods for a particular situations by providing scenario-specific authentication factors.

IV. Continued Flexibility

Motorola Solutions recommends NIST ensures continued flexibility in the CSF going forward. Continued flexibility in the CSF is paramount to ensuring that entities of all sizes can leverage the CSF in a manner that best suits their risk profile/ tolerance and customer needs.