The current NIST resources “Framework for Improving Critical Infrastructure Cybersecurity (CSF)” and the variety of existing and potential standards, guidelines, and other information that includes Cybersecurity Supply Chain Risk Management is not always comprehensive enough to cover the many use cases that arise:

a) outside the critical infrastructures these NIST resources were originally designed to address,
b) from the pervasive programmability of logic-bearing HW and SW systems and networks that in unison provide and deliver advantages for national interests, and
c) as a result of the difficulty of gaining visibility on opportunities for malice, compromise, or sabotage at any point in the extended supply chains of providers, performers, and development, operations, or sustainment infrastructures.

The attached comments are provided as input to enhance comprehensive coverage to a whole of government perspective for NIST resources.

Michele Iversen
Director, Risk Assessment & Operational Integration
DOD CIO Cybersecurity
[redacted]

DoD comments are:

- A resolution and harmonization between Cyber-SCRM and ICT SCRM would improve both the CSF and the proposed National Initiative for Improving Cybersecurity in Supply Chains (NIICS). Cyber-SCRM and ICT-SCRM are often conflated, and possibly confusing to the full scope of users of NIST resources.
    - ICT, and its supply chain risk management, as codified in various NDAA sections, is used in Executive Orders, and defined in U.S. Code. When taking an acquisition action, such as an exclusion, it's important that the reference to ICT conform to the authorizing legislation, which cites ICT. From a risk management perspective, DoD must identify and mitigate risks of information technology from any and all logic-implementing or associated devices or technologies, from microelectronics to commercial services.
    - C-SCRM, as an engineering construct, has value by invoking mandatory RMF Controls.
    - C-SCRM separates other uses of ICT, such as when used in OT or within DoD NSS, ICT are often embedded in platforms, and the distinction for OT is often not germane to the system's security engineering function.
    - The use of RMF as a minimum/initial requirement for NSS development is highly dependent and inter-related to the NSS architecture which often requires multiple iterations, as the systems' designs mature for the multiple systems , and is a different problem set from the selection of controls that should be tailored to the use of ICT within Critical Infrastructure by Departments and Agencies..
    - NIST resources should focus on deeper analysis of uncertainties that inform but also distinguishes the risks of ICT as used in infrastructure versus some key characteristics of use of ICT products, and services in NSS, systems-of systems as constituent elements of NSS systems, platforms; and cyberspace as a warfighting domain. This addresses the unique uncertainties of missions and mission systems and networks from the different, but important uncertainties of implementing ICT components (products, services, and infrastructures).
    - Analyses of these uncertainties and adversarial opportunities should include full supply chain assessment (n-tier), system's security engineering and Red Teams, forensics, if it's a critical system, and advanced monitoring for network-based systems.

- The Framework was initially developed for Critical Infrastructures.
    - A comprehensive capstone resource should be developed. This would allow the types of uncertainties expressed above to be separately assessed and the analyses to focus on the integrated view of risk.
        - This would avoid simply stretching of existing NIST resources to include all networks, and DoD weapons systems.
        - This would acknowledge that residual risk (uncertainties) from integrating multiple differing risks is the overarching concern of leadership and users of systems and networks fabricated, operated and sustained with ICT.
    - The current practice of Departments and Agencies developing their own Overlays results in variability, which may not expose the risks to other Departments and Agencies. The individual Department or Agency may be operating at low risk to their mission w/o realizing how others may be impacted by the residual risks that they manage. COOP/COG and other whole-of-government activities (National Security, National Commerce, etc.) need a capstone resource to enable integrated risk assessments grounded in the broader/shared uncertainties associated with observation and

measurement (NIST's core competency), particularly for their common operating space of ICT, cyber and cyber-security.

- The RMF structure that advocates for the selection of the controls, is agnostic to the type of system and network being developed, and in some cases, the lifecycle phases of the system or network. The users of NIST resources need a CSF that works for both development of new capabilities as well as maintaining existing networks and systems upgrades.
    - There is no NIST capstone resource that addresses the full life-cycle of the use, operations, and sustainment of cyberspace and the ICT that implements cyber.
    - Application of existing or only incrementally improved NIST resources focused on Critical Infrastructure, and repurposed without recalibration exacerbates the sub-optimal management of risk for National Interests by NOT providing an integrated risk assessment that ties together the collective uncertainties and managed risks of individual Departments and Agencies, and the specific capabilities that are intended to function as an integrated whole or have otherwise unseen dependencies on other managed risks, e.g. COOP and Continuity of Government.

- Enhance Section 3.3 (Communicating Cybersecurity Requirements with Stakeholders) to account for the likelihood that individual organizations may enforce varying and conflicting Cybersecurity, including those related to the supply chain, requirements. Integrate the guidance, for addressing this concern, provided in NIST SP800-161 Rev. 1.

- Enhance Section 4.0 (Self-Assessing Cybersecurity Risk with the Framework) to integrate guidance on how SP800-30 Rev. 1 can be leveraged to perform the risk measurement to assign a value. It appears that the CSF depends on measuring, or assessing risk, but avoid alignment to the NIST standard commonly used to assess cybersecurity risks.

- Update the links to the Security Controls using the latest updates in SP800-53 Rev. 5

- Update globally to remove critical infrastructure centric language since the framework can be applied in scenarios beyond those within the critical infrastructure community.