CISA Cybersecurity Performance Goals – Comments from CSCC

The baseline cybersecurity performance goals should align with the NIST Cybersecurity Framework.

The NIST Cybersecurity Framework (CSF) developed in 2014 has proven to be one of the most widely adopted best practices for cybersecurity. The NIST CSF is designed around five core functions – Identify, Protect, Detect, Respond, and Recover. The CISA cybersecurity performance goals should be aligned with specific categories of the NIST CSF to ensure cybersecurity practices and postures by owners and operators of critical infrastructure do not conflict with the NIST Cybersecurity Framework. Furthermore, the Framework Implementation Tiers used within the CSF are very useful to scale to the size of the organization while fostering a risk-based evaluation rather than checkbox compliance.

The baseline cybersecurity performance goals should be outcome based.

The baseline cybersecurity performance goals should be flexible and outcome based. The goals should not be prescriptive in how to achieve desired outcomes because prescriptive requirements can quickly become outdated and hinder effective solutions. Rather, each goal should define or describe the desired outcome as a means to provide guidance to owners and operators of critical infrastructure, so that they may determine the best means of execution to achieve the stated goal. One size does not fit all, and each owner and operator is unique. Therefore, the activities required to achieve the goal will vary with each owner and operator.

The baseline cybersecurity performance goals' objectives are outcomes and not objectives and should be part of the goal itself.

The baseline cybersecurity performance goals should only have one element – the performance goal. Decomposing the goals into three elements – performance goal, objectives, and sample evidence of implementation – makes it difficult for owners and operators of critical infrastructure to tailor their cybersecurity programs to meet the goal. Further, by decomposing the goal to include objectives and sample evidence can lead to conflicts with other existing cybersecurity and information security standards and NIST publications.

We understand and appreciate CISA's desire to include a level of specificity as a means to providing guidance for how to achieve the goal. For those cases where the objective is the true goal CISA should restructure and re-state the objective as a non-prescriptive goal itself.

And finally, all the goals should be structured as singletons and not compound goals to allow for better monitoring of success toward achieving the goals.

The baseline cybersecurity performance goals should be forward looking.

As part of developing performance goals about cybersecurity practices and postures, the goals should be forward looking to avoid tasking owners and operators with reworking existing systems or architectures. Owners and operators, as part of updating their cybersecurity practices and postures, should have the latitude for how they can and will improve the cybersecurity of their incumbent systems or architectures that they have deemed through self-risk assessments need to be improved.

CISA should take additional steps to gather input from industry partners.

The leadership of numerous critical infrastructure sectors have called on CISA to extend the comment period for its performance goals. We urge CISA to use such additional time to engage industry more deeply on these important topics and receive feedback from SMEs in the private sector. For instance, CISA may consider hosting a workshop on the performance goals.

Specific recommendations.

While urging CISA to take the steps recommended above, we also wish to highlight the line-by-line comments developed by CTIA on specific aspects of the current document. These comments should be considered as part of the broader set issues that CISA should seek to address, as detailed in this letter.

What specific changes are needed to ensure the goals and objectives are clear and actionable for stakeholders in your sector or subsector?

Any cybersecurity performance goals identified through this exercise, to be clear and actionable to all stakeholders, must account for the needs and finite capabilities of small and mid-sized providers ("SMBs"). This is not to suggest SMBs should be held to a different or lesser standard, but rather, the goals must be flexible enough to allow SMBs the ability to meet them while also written in terms capable of being understood and implemented by individuals without an engineering or cybersecurity background. SMBs often do not have trained cybersecurity or IT professionals to manage their companies' cyber practices or the financial ability to purchase hardware, software or cloud-based tools intended to decrease companies' cyber risk. Additionally, any goals must be adaptable to the individual needs of each provider as there is no one size fits all solution to cybersecurity, regardless of the provider's size. The NIST CSF accomplishes this objective due to the CSF's ability to be scalable depending upon the needs and capabilities of each company, while avoiding a checklist that does little to advance a company's cybersecurity posture.

How can the goals and objectives be improved to better capture the cybersecurity practices needed to ensure the safe, secure, and reliable operation of infrastructure across sectors and subsectors?

The National Security Memorandum directs the Secretary of Homeland Security to issue cybersecurity performance goals applicable to all critical infrastructure providers, regardless of

sector or size. Suggesting SMBs should implement procedures that often require a significant financial investment as well as a large team of highly trained employees, however, is not feasible. The ICT Supply Chain Risk Management Task Force ("Task Force") recognized the need to adapt existing cybersecurity resources and guidance to the needs of small and mid-sized IT and communications providers when the Task Force created the Small and Medium-Sized Businesses Working Group for the communications and IT sector in 2021. Similarly, NTIA recently established the Communications Supply Chain Risk Information Partnership (C-SCRIP) "to improve small and rural communications providers' and equipment suppliers' access to information about risks to key elements in their supply chain." Any goals developed pursuant to this exercise should continue to allow for the distinct needs and capabilities of SMBs.