Before the Department of Homeland Security
Cybersecurity and Infrastructure Security Agency
Washington, D.C.

In the Matter of	)	
	)	
Cross-Sector Cybersecurity Performance Goals and Objectives	)	Draft Common Baseline Version 2.0 Controls List June 2022
	)	
	)	

COMMENTS OF CTIA – THE WIRELESS ASSOCIATION, NCTA – THE INTERNET & TELEVISION ASSOCIATION, and USTELECOM – THE BROADBAND ASSOCIATION

Tom Power
Senior Vice President and General Counsel

Loretta Polk
Vice President and Deputy General Counsel

Paul Eisler
Senior Director, Cybersecurity

Tom Sawanobori
Senior Vice President and Chief Technology Officer

CTIA – The Wireless Association
1400 16th Street, NW, Suite 600
Washington, DC 20036

NCTA – The Internet & Television Association
25 Massachusetts Avenue, NW – Suite 100
Washington, D.C. 20001

USTelecom – The Broadband Association
601 New Jersey Avenue, NW, Suite 600
Washington, DC 20001

August 15, 2022

Table of Contents

I. INTRODUCTION

CTIA – The Wireless Association,[1] NCTA – The Internet & Television Association,[2] and USTelecom – The Broadband Association[3] (collectively, "the Associations") appreciate the opportunity to comment on the Department of Homeland Security ("DHS") Cybersecurity and Infrastructure Security Agency ("CISA") Draft *Common Baseline Version 2.0 Controls List* ("Draft Controls List"),[4] which will be incorporated into the forthcoming draft *Cross-Sector Cybersecurity Performance Goals Common Baseline Version 2.0 Full Document* ("Common Baseline"). This effort arises out of the National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems ("Control Systems Memorandum"), which envisioned a "voluntary, collaborative effort between the Federal Government and the critical infrastructure [("CI")] community to significantly improve the cybersecurity of control systems," and directed DHS to issue "[C]ross-[S]ector [C]ontrol [S]ystem [G]oals."[5] The

[1] CTIA – The Wireless Association® (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st-century connected life. The association's members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry, and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[2] NCTA – The Internet & Television Association is the principal trade association of the cable television industry in the United States, which is a leading provider of residential broadband service to U.S. households. Its members include owners and operators of cable television systems serving nearly 80 percent of the nation's cable television customers, as well as more than 200 cable program networks.

[3] USTelecom – The Broadband Association is the premier trade association representing service providers and suppliers for the broadband industry. Its diverse member base ranges from large publicly traded communications corporations to local and regional companies and cooperatives—all providing advanced communications services to both urban and rural markets.

[4] Draft Cross-Sector Cybersecurity Performance Goals (CPGs) Common Baseline: Controls List, CISA (June 23, 2022), https://www.cisa.gov/sites/default/files/publications/Common_Baseline_v2_Controls_List_508c.pdf ("Draft Controls List").

[5] Memorandum, The White House, National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems (July 28, 2021), https://www.whitehouse.gov/briefing-room/statements-

Associations appreciate CISA's commitment to working with the private sector to develop the Controls List that will be incorporated into the Common Baseline and to prepare for the development of sector-specific performance goals.

The Communications Sector has long partnered with DHS and CISA to remain on the cutting edge of cybersecurity practices, and it invests significant resources securing the nation's communications networks. The Associations and their members share CISA's goal to continually improve cybersecurity in the face of dynamic threats.

There has been substantial progress in enhancing the nation's overall cybersecurity across CI sectors—and more broadly among industry writ large—since release of the National Institute of Standards and Technology's ("NIST") Cybersecurity Framework ("CSF"). That progress is a direct result of the voluntary nature of the CSF, its focus on taking a risk-based approach to cybersecurity, and its emphasis in providing organizations with considerable flexibility to use it. Our broad concern is that the Draft Controls List represents a departure from these key attributes that continue to drive progress on—and enhancement of—cybersecurity across the nation. Performance goals should be outcome oriented, and to that end, CISA should establish the broad security outcomes that CI owners and operators should be striving to achieve, but refrain from directing specific means to achieve those outcomes. Accordingly, with these comments, we encourage CISA to:

- Re-cast performance goals in terms of security outcome objectives rather than as prescriptive controls. A flexible and risk-based approach to the Common Baseline, rather than a checklist of controls, is more appropriate and will be more effective.
- Ensure that the Common Baseline is more firmly rooted in principles of risk management. CISA should encourage CI owners and operators to start with a risk assessment, and then the Common Baseline should present a catalog of controls that can

releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/ ("Control Systems Memorandum").

be customized to match an organization's business or mission needs and risk profile.

- Revise controls that are overly prescriptive and not appropriate for all CI sectors. When drafting its menu of controls, CISA should ensure that the controls are broad and adaptable enough to address different risks and maturity levels of various CI sectors, as well as diverse owners and operators within the same CI sectors.
- Reiterate the important differences between and among CI sectors. To account for this diversity, CISA should ensure that flexibility is a driving goal as each Sector Risk Management Agency ("SRMA") begins to develop its sector-specific goals.
- Further align the Common Baseline with the CSF, as well as other cybersecurity efforts.
- Focus the Common Baseline's on CI control systems, consistent with the Control Systems Memorandum.

The Associations appreciate the opportunity to work with DHS and CISA to strengthen the nation's cybersecurity posture. We welcome continued collaboration, including a meeting to discuss this feedback, as CISA finalizes the Common Baseline.

II. THE COMMON BASELINE SHOULD DRAW FROM LONGSTANDING PRINCIPLES OF RISK MANAGEMENT.

A. The Common Baseline Should Be a Framework that Helps a CI Control System Owner or Operator to Select and Tailor Controls Appropriate to the Organization's Risk.

CISA should adjust the Common Baseline to better accomplish its requirements under the Control Systems Memorandum and to better align with principles of risk management. The Control Systems Memorandum directs CISA to establish "performance goals;"[6] however, the Draft Controls List includes specific and prescriptive controls. While it is promising that the Draft Controls List makes clear that the controls are not intended to be either compulsory or comprehensive,[7] CISA should take steps to clarify and ensure that the Common Baseline is flexible and outcome-based—two foundational risk management principles.

A flexible and outcome-focused approach—which can be tailored for a range of

[6] *Id.* § 4.

[7] *See* Draft Controls List at 2.

organizations across CI sectors of varying types, sizes, and maturity—is the most effective way to promote cybersecurity for CI control system owners and operators. This type of risk-based approach enables organizations to keep pace with changing technology and stay ahead of bad actors. On the other hand, overly prescriptive controls run counter to established risk-management principles and will work against efforts to promote cybersecurity. An unduly prescriptive or "check-the-box" approach is counterproductive, as it leads to a compliance mindset and provides a roadmap for bad actors. Additionally, a detailed list of specific requirements will quickly become outdated, ineffective, and obsolete. For example, as bad actors have increasingly turned to phishing to harvest credentials, cyber best practices have evolved beyond password complexity requirements toward multi-factor authentication ("MFA").[8] Static guidance on password complexity would have failed to react to this development and protect against novel threats.

For these reasons, longstanding and effective cybersecurity frameworks and guidance have embraced a risk-based approach, as opposed to a "one-size-fits-all" solution to improve cybersecurity in a variety of settings. NIST's seminal CSF is the clearest example. It presents a "set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors."[9] NIST makes clear that the document "is not a checklist of actions to perform," but rather that "[i]t presents key cybersecurity outcomes identified by stakeholders as helpful in managing cybersecurity risk."[10] When using the CSF, "an organization

[8] *See CISA Challenges Partners and Public to Push for "More than a Password" in New Social Media Campaign*, CISA (June 6, 2022), https://www.cisa.gov/news/2022/06/06/CISA-Launches-Morethanapassword#:~:text=CISA's%20More%20Than%20a%20Password,passwords%20reused%20from%20other%20systems.

[9] Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, NIST at 3 (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf ("CSF Version 1.1").

[10] *Id*. at 6.

can review all of the Categories and Subcategories and, based on business/mission drivers and a risk assessment, determine which are most important; it can add Categories and Subcategories as needed to address the organization's risks."[11] The CSF also defines steps for establishing or improving a cybersecurity program, which includes conducting a risk assessment.[12]

There are multiple other examples of outcome-focused NIST tools that embody a risk-management approach. NISTIR 8259A, NIST's *IoT Device Cybersecurity Capability Core Baseline* ("NIST IoT Cyber Baseline") is a prime example of a non-prescriptive, risk-based, and outcome-oriented baseline. It states, "[t]he individual capabilities in the baseline may be implemented in full, in part, or not at all. It is left to the implementing organization to understand the unique risk context in which it operates and what is appropriate for its given circumstance."[13] Another example is the AI Risk Management Framework, which NIST is developing. There, NIST is striving for the document to "[b]e outcome-focused and non-prescriptive. The Framework should provide a catalog of outcomes and approaches rather than prescribe one-size-fits-all requirements."[14]

CISA should review these documents to ensure that the Controls List reflects years of risk management best practices. In line with the examples above, CISA should ensure that the Common Baseline is not simply a list of rigid controls, but instead is a practical tool for CI control system owners and operators to customize based on their unique contexts. The Common Baseline is intended to be "broadly applicable" to the CI community—an audience composed of

[11] *Id*. at 4.

[12] *See id*. at 14-15.

[13] NISTIR 8259A, IoT Device Cybersecurity Capability Core Baseline, NIST at 1-2 (May 2020), https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259A.pdf ("NISTIR 8295A").

[14] AI Risk Management Framework: Initial Draft, NIST at 3 (Mar. 17, 2022), https://www.nist.gov/system/files/documents/2022/03/17/AI-RMF-1stdraft.pdf.

entities with diverse functions, sizes, and existing cyber practices and policies.[15] To truly be applicable to this broad audience, the Common Baseline should be drafted to define *what* common goals should span across CI sectors, leaving the specifics of *how* to implement those goals to individual CI control system owners and operators.

A core theme that CISA should make clear throughout the Common Baseline is that approaches across CI organizations can and should vary, and likewise, approaches can and should evolve as risks change. Specifically, the Common Baseline should make clear that the starting point for its numerous and diverse users should be a risk assessment, which will allow for development of a tailored cybersecurity approach, consistent with CISA's broad goals, that meets the unique needs of an individual organization. Based on this risk assessment, CI control system owners and operators should then select and/or tailor the controls in the Common Baseline, as appropriate to the organization's own sector and needs. CISA's final Common Baseline should make this process explicit, ensuring that the Controls List is essentially a menu of options for CI owners and operators to select from and tailor, and not a compliance checklist.

B. CISA Should Adjust Specific Controls that Are Too Prescriptive, Ensuring that the Common Baseline's Controls Are Flexible Enough to Address Different Risks and Maturity Levels Across CI Sectors.

CISA should revisit certain controls in the Draft Controls List because, as drafted, they are overly prescriptive, too narrow, and not rooted in risk management. In particular, CISA should revisit the draft controls listed in Table 1 below.

[15] Draft Controls List at 2.

Table 1

Control	Draft Text	Feedback
3.2	"All data, both in transit or at rest, should be encrypted to ensure confidentiality in both IT and CS. Owners/operators should verify that data is encrypted by a suitably strong algorithm. Additionally, any assets incapable of using suitable encryption should be prioritized for upgrade or replacement."[16]	The reference to "all data" is remarkably overbroad. Encryption is not always appropriate for all data at rest or in transit, and encryption creates tradeoffs for network and data management, usability, and size constraints. Looking ahead, there are complexities around post-quantum cryptography that may factor into an organization's risk assessment regarding encryption. Encryption also requires key management for the lifecycle of data and systems that are encrypted. To protect data, organizations can take other appropriate measures, depending on the specific context or the organization and its data. At a minimum, CISA should update its language in two ways. • *First*, CISA should clarify that not all data presents the same risk or requires identical security approaches. CI owners and operators may have important system data that reasonably should be secured with encryption. But these same owners and operators can also have website, email, marketing, regulatory, purchasing, business, and other data that is less appropriate for mandatory encryption. Organizations should assess several factors—including data's sensitivity, purpose, and location (e.g., backup data), as well as the type of network and network architecture level, among other things—when determining an optimal way to secure data. • *Second*, CISA should broaden the options for protecting data beyond encryption. CISA could call for "encryption or other protections, as appropriate."
5.1	"Owner/operators should patch all Known Exploited Vulnerabilities in all public facing systems to reduce the risk of defense evasion by threat actors. Asset owners should validate that the KEV's	This draft control, too, is overly prescriptive and does not factor in the complexities associated with operational technology ("OT"), which should be the focus of the Common Baseline, as discussed below. While vulnerability management is an important part of an organization's cybersecurity approach, patching all vulnerabilities is not always appropriate and, in many

[16] *Id.* at 8.

Control	Draft Text	Feedback
	listed at Known Exploited Vulnerabilities Catalog | CISA are patched within the designated timeframe. When patching is not feasible, compensating controls should be applied and documented."[17]	OT scenarios, can cause unintended consequences and have adverse implications. As NIST has explained with respect to industrial control systems: "A patch may remove a vulnerability, but it can also introduce a greater risk from a production or safety perspective. Patching the vulnerability may also change the way the OS or application works with control applications, causing the control application to lose some of its functionality."[18] These effects could be deleterious in the CI environment, putting the control as drafted in tension with the "do no harm" principle. In short, patching should not be pursued blindly in every case. CISA should update this control as follows: • *First*, while the Associations appreciate that the draft control recognizes that patching is not always feasible, we urge CISA to build on that statement and broaden the vulnerability management control even more, with the final control recommending mitigating Known Exploited Vulnerabilities, which may include patching or other compensating controls. • *Second*, CISA should point CI control system owners and operators to the broad range of vulnerability resources, which includes but is not limited to CISA's KEV Catalog.
1.3	Draft Control 1.3 states that "[a] minimum password strength should be maintained on all IT and OT assets technically capable of sufficient password protection . . . ."[19] It describes the associated measurement as a "system-enforced policy that mandates a minimum password length (generally 12 or more	This control should not point CI owners and operators only to password protection, but, instead, the control should discuss the context of the broad set of Authenticator Assurance Levels available to organizations to address brute force attacks and other risks to account security. There are multiple options available that can obviate the need to place password controls on "all" IT and OT assets technically capable of password protection. Consistent with a risk-based approach to security, organizations should have the flexibility to employ these other options, such as various forms of MFA, out-of-band devices, and

[17] *Id.* at 12.

[18] NIST SP 800-82 Rev. 2, Guide to Industrial Control Systems (ICS) Security, NIST at 6-40–41 (May 2015), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf ("NIST SP 800-82 Rev. 2").

[19] Draft Controls List at 3.

Control	Draft Text	Feedback
	characters)."[20]	single-factor one-time password devices, which in many instances will subsume a password approach. Also, where password protection is employed, the Common Baseline should not prescribe the password's specific length or other characteristics. If the draft control does include details on password length, it should make clear that its discussion is only an example of a minimum password length, and it should use the example of eight characters, which is consistent with NIST's Digital Identity Guidelines.[21]
1.4	"Phishing resistant MFA should be implemented to reduce the risk of initial access and credential access attacks on. This control should be verified by the enrollment of all IT user accounts in MFA. For control systems assets, MFA should be enabled whenever possible, especially where remote access is being utilized, as well as all engineering workstations and HMIs."[22]	The Associations agree that, overall, MFA is an important tool. As with any other cybersecurity tool or approach, however, it should be deployed in a risk-informed manner. CISA should not be overly prescriptive about appropriate types of MFA that should be used. No one method will address all security concerns, and an appropriate MFA method will depend on the nature and the sensitivity of the information being accessed, among other considerations that should be assessed by the organization based on its environment.
2.1	Draft Control 2.1 states that only "approved" hardware, firmware, and software may be installed on all IT and OT assets to reduce malware risks.[23]	CISA should clarify that it is the owner/operator that should approve installations,[24] as appropriate, informed by the organization's specific context and risk.
2.4	"Owner/operators should develop and maintain accurate documentation identifying baseline network topology and OT device configuration information to aid in both	The Associations agree that this an appropriate general goal, but the Common Baseline should acknowledge that some operators may have some legacy infrastructure for which this draft control is not practical. It should include language that makes clear that in certain circumstances, owners/operators may

[20] *Id.*

[21] NIST SP 800-63B, Digital Identity Guidelines: Authentication and Lifecycle Management, NIST at § 5 (June 2017), https://pages.nist.gov/800-63-3/sp800-63b.html.

[22] Draft Controls List at 4.

[23] *Id.* at 6.

[24] *See id.* at 10 (specifying that owners/operators should designate leadership for IT and OT cybersecurity as well as an accountable party for OT cybersecurity).

Control	Draft Text	Feedback
	management and restoration activities. Cybersecurity managers must confirm the existence of this documentation, and institute a codified process to update this as necessary."[25]	reasonably employ other mitigation techniques. Indeed, it would be helpful for CISA to generally make this point clear, with respect to all of its draft controls.
5.5	"Owner/operators should conduct adversary emulation (e.g., red team and/or purple team) testing on an annual basis to identify vulnerabilities across all IT and OT assets, and remediate any identified issues as soon as possible. Organizations should confirm that they conduct such tests on a recurring basis not to exceed 24 months between exercises, and that identified vulnerabilities are addressed in manner so as to be confirmed as resolved future testing."[26]	CISA should frame this control as a more general goal rather than a prescriptive executional control. CISA can look to and reference CSF ID.RM and ID.RA, which would help solidify this control as goal oriented. The reference to "all IT and OT assets" is particularly overbroad for the Communications Sector to the extent "OT assets" includes internal-facing ports associated with the provision of network services. The nature of the Communications Sector is such that a single service provider may have hundreds of thousands or millions of ports, the vast majority of which are internal-facing. For communication service providers, that scale necessitates a risk-based approach to adversary emulation testing. Consistent with risk-informed mitigation principles, penetration testing activities will generally cover external-facing vulnerabilities and a subset of internal-facing ones that present the greatest network risks.
6.1–6.3	Draft Control 6.1 recommends that CI owner/operators include security capabilities as evaluation criteria for IT and OT asset procurement;[27] and Draft Controls 6.2 and 6.3 advise that owner/operators should require IT or OT vendors or service providers to notify them of security incidents, breaches, or vulnerabilities "in a reasonable timeframe."[28]	The Associations support responsible vendor management and vulnerability disclosure and have been active in many supply chain security efforts. But these controls are drafted in a very broad and compulsory way; instead they should be framed as general goals rather than prescriptive requirements. For example, the general goal could include conducting supply chain risk management assessments to identify critical network components and mitigate procurement of assets with unsatisfactory cybersecurity practices. CISA can encourage appropriate contractual requirements to facilitate disclosures and cooperation between parties, without being so prescriptive.

[25] *Id.* at 7.

[26] *Id.* at 13.

[27] *See id*. at 15.

[28] *Id*. at 15-16.

Control	Draft Text	Feedback
		As drafted, these draft controls would present a risk of unintended harmful consequences. For example, Draft Control 6.3 appears to require owners/operators to require vendors to disclose "any" vulnerabilities that exist,[29] without qualification. New vulnerabilities may be found regularly across diverse and numerous systems, so an overly broad disclosure obligation could become chaotic, with a flood of disclosures that in many instances are not actionable for the CI owner or operator. Disclosure could result in exploitation of the vulnerabilities to the extent that vendors are pushing out disclosures to large groups of customers and therefore become known to bad actors. Also, without a patch or other mitigation for the vulnerability, this in many instances would not reduce risk. Additionally, in general, CISA should avoid language in the controls that would appear to create procurement requirements. Organizations are in the best position to address their unique and complex cybersecurity and procurement needs and capabilities; specific procurement requirements could be overly burdensome, duplicative, or unnecessary for many organizations that have established procurement processes. Specifically, regarding draft control 6.1, it is unclear how language in procurement documents would achieve the intended goal unless owners/operators were to include in flow-down clauses to sub-tier vendors. For example, if a vendor procures a product in support of a CI owner or operator, the owner or operator would need to include language that states the vendor must choose one that demonstrates a stronger security posture. In addition, the phrase "roughly equivalent" is subjective.[30] A more reasonable formulation would be: "Assets and Services are evaluated with regards to security posture. Given two roughly equivalent products or services in terms of function or cost, the one that demonstrates a stronger security posture will be evaluated higher."

[29] *Id.* at 15 ("Owner/operators should require that all IT or OT vendors or service providers notify them of any security vulnerabilities in a reasonable timeframe to reduce the risk of threat actor exploitation. Organizations should include contract clauses in all procurements or SLA's stipulating said notification.").

[30] *See id.* ("Language in procurement documents that, given two roughly equivalent products or services in terms of function or cost, the one that demonstrates a stronger security posture will be evaluated higher.").

Control	Draft Text	Feedback
7.1	"Owners/operators should report cybersecurity incidents across IT and OT assets to CISA, as well as any other mandatory reporting stakeholders for each organization, as soon as possible to minimize the impact of threat activity internally and enhance community ability to position to meet emerging or active threats. The control shall be validated by the presence of codified policy and defined procedure on how and to whom to report incidents."[31]	The Associations support voluntary information sharing to better strengthen and coordinate cybersecurity efforts. While reporting and information sharing can be helpful, there are some circumstances where it may be inappropriate to report incidents to a wide range of stakeholders in a specific time frame. In addition, it is premature to codify an expectation for all CI owners and operators to report all incidents to CISA; CISA has not set out its approach to implement CIRCIA and the agency should wait and harmonize this control with its future regulations. CISA should make clear that existing incident reporting requirements—which are expanding and overlapping across the federal government—can vary from one sector to another. The agency can note the existence and possible application of mandatory incident reporting, and encourage those subject to such obligations to have a clear policy for how and to whom such reporting will be handled.
8.2	"All owner/operators should implement segmentation between IT and OT networks to prevent initial access by threat actors. Organizations should verify that devices on either side of segmentation lines/safety zones must not connect to the opposite side with minimal exceptions and only through a correctly configured firewall or comparable alternative."[32]	This draft control is overly prescriptive and oversimplifies the tradeoffs in segmentation for varied networks; segmentation can be costly and can impede access to business or mission-critical applications. An overly rigid expectation for default segmentation would deprive organizations of the capability to manage their systems and networks. Accordingly, at a minimum, CISA should remove language like "must."

[31] *Id.* at 17.

[32] *Id.* at 19.

III. CISA'S GUIDANCE SHOULD TAKE INTO ACCOUNT THE DIVERSITY OF CI OWNERS AND OPERATORS.

To be a useful tool and truly span all CI sectors, the Common Baseline must acknowledge the diversity of organizations to which it will be relevant, and it should be explicit that each CI sector may use the guidance in unique ways. To start, there are important differences between—and even within—CI sectors, which have individualized considerations that should be recognized in the Common Baseline. For example, different CI sectors may be at different cybersecurity maturity levels. In many respects, the Communications Sector has a mature posture that is at the cutting edge of cybersecurity innovation. Further, each sector has unique considerations. As mentioned above, in the Communications Sector, owners and operators can be service providers, so in addition to operating their own network, they provide communications and network services to third party enterprises. The scale and complexity of network architectures across the Communications Sector based on this unique feature warrants unique approaches to cybersecurity.

Moreover, there are differences within sectors. For example, within the Communications Sector, each segment—including broadcast, cable, satellite, wireless, and wireline—has unique considerations, in part due to each segment's unique operating environments. As an example of the Communications Sector's longstanding leading role on cyber issues and the differences among the subsectors, soon after the CSF version 1.0 was developed, the Communications Sector came together in the Federal Communications Commission's ("FCC") Communications Security, Reliability, and Interoperability Council ("CSRIC") to conduct a comprehensive

mapping of the NIST CSF for each of the industry's subsectors.[33]

Additionally, each organization within various sectors and segments has a unique risk profile and context to consider in developing an appropriate cybersecurity posture. Again, with respect to the Communications Sector as an example, there is a rich diversity of operators—as illustrated by the diversity of the Associations' own membership.

These differences are acknowledged and accounted for in a wide range of CI cybersecurity resources. The Control Systems Memorandum recognizes the important differences between sectors, stating that "Cybersecurity needs vary among critical infrastructure sectors, as do cybersecurity practices."[34] Other resources, such as the CSF, recognize and account for these differences as well.[35] Indeed, striking the right balance between developing goals for all users while still building in flexibility can be challenging, but it is doable. For example, the NIST IoT Cyber Baseline sets outs to create a baseline, but it acknowledges that not every element of the baseline will be applied similarly—if at all—depending on context.[36]

Accordingly, the varying attributes across CI sectors should be factored into the Common Baseline's guidance. *First,* at a minimum, the Common Baseline should be re-drafted to be broader and more flexible, as detailed above. This will ensure that it can account for various implementations. *Second,* CISA should make this intended flexibility explicit, explaining that

---

[33] *See generally* CSRIC IV, Working Group 4, Cybersecurity Risk Management and Best Practices, Final Report, FCC at 4-5 (March 2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf ("CSRIC Report").

[34] Control Systems Memorandum § 4.

[35] CSF Version 1.1 at *vi* ("The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances. . . . To account for the unique cybersecurity needs of organizations, there are a wide variety of ways to use the Framework.").

[36] NISTIR 8295A at 3 ("The core baseline's role is as a default for minimally securable devices. However, device cybersecurity capabilities will often need to be added or removed from an IoT device's design, integration, or acquisition to best address an organization's common cybersecurity risks.").

the Common Baseline should be tailored for each sector and organization, and will be applied differently based on those different contexts. *Third*, the Common Baseline should be more explicit that the applicable SRMA should tailor the Baseline for each sector as part of the sector-specific goals, and that such sector-specific guidance will need to be flexible, to account for specific organizations' unique cybersecurity needs.

IV. THE COMMON BASELINE SHOULD BUILD ON EXISTING RESOURCES AND PROVIDE GUIDANCE ON PRACTICAL IMPLEMENTATION.

A. NIST's CSF Should Be the Foundation for the Common Baseline.

As described above, NIST has a long history of developing risk-based guidance, in collaboration with CI sectors and other stakeholders, with the most notable example being the CSF. The Associations appreciate CISA's incorporation of references to the CSF in its Draft Controls List; however, more is needed for true alignment that will leverage the CSF and the multitude of cyber tools that have been built upon the CSF's foundation.

To more fully align the Common Baseline and the CSF, CISA should take the following steps:

- CISA should mirror the five functions of the CSF—with flexible and outcome-based control system goals mapped to Identify, Protect, Detect, Respond, and Recover. The current categories of controls in the Draft Controls List are not clearly aligned with the CSF's functions. Lack of alignment with the CSF's approach to cybersecurity risk management will make CISA's document difficult to incorporate into well-established and mature cyber programs that many owners and operators across CI—including those in the Communications Sector—already have established, consistent with the CSF.
- CISA should explicitly describe how the Common Baseline and the CSF interact, making clear that the final Common Baseline should not be used alone, but instead, should be layered on top of the CSF. This will help CI owners and operators that conform to the CSF to more efficiently integrate the Common Baseline into their CSF-based cybersecurity approach.
- CISA should also echo the CSF's language regarding voluntary and flexible use. This will avoid any confusion around the voluntary nature of the Common

Baseline,[37] and also will serve as a guidepost for any policymakers who may look to the Common Baseline as a reference point.

Further, CISA's document should reflect the fact that the CSF "is a living document" that NIST continues to update.[38] The current version of the CSF is Version 1.1; however, NIST is in the process of updating the CSF with a Version 2.0.[39] The Common Baseline should align with the most up-to-date CSF, and avoid creating different structures or approaches that may duplicate effort. CISA should coordinate with NIST as CISA develops the Common Baseline and as NIST develops CSF Version 2.0 so that the workstreams can inform each other.

B. CISA Should Incorporate Additional Cybersecurity References and Resources into the Common Baseline.

The Controls List should include additional "External Reference" resources beyond the CSF and the ISA/IEC 62443 standard on security capabilities for control system components. Again, as a guiding example, NIST's CSF lists a range of Informative References for its Categories and Subcategories under each Function. CISA should also include NIST's compendium of OT Security Organizations, Research and Activities included in draft NIST SP 800-82, Rev. 3, which highlights several industry-led consortia and standards, including the Institute of Electrical and Electronics Engineers, Inc. and the International Organization for Standardization.[40] In addition, CISA could reference the extensive cybersecurity tools and documents that have been developed for the CI Communications Sector, such as the CSRIC

[37] Draft Controls List at 2 ("The CPGs are not: . . . Compulsory[.] National Security Memorandum-5 does not create new authorities that compel owners and operators to adopt the CPGs or provide any reporting regarding or related to the CPGs to any government agency.).

[38] CSF Version 1.1 at *vi*.

[39] *See Updating the NIST Cybersecurity Framework – Journey to CSF 2.0*, NIST (last updated July 18, 2022) https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20.

[40] Draft NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security, NIST at Appendix D (Apr. 2022), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.ipd.pdf ("Draft NIST SP 800-82 Rev. 3").

Working Group Report on CSF implementation guidance for each of the five key segments of the industry.[41] These resources should be incorporated as examples into the Common Baseline, and CISA should consider adding references that other CI sectors have developed, as well.

C. CISA Should Help Illuminate How the Controls List Can Be Used.

In addition to the NIST cyber resources highlighted throughout these comments, CI stakeholders may also be working to align their practices with the guidance in other cybersecurity resources, including NIST Special Publication 800-171, which covers security requirements for protecting the confidentiality of Controlled Unclassified Information; international security standard frameworks such as ISO/IEC 27001;[42] and other baseline documents. The Draft Controls List stands to overlap—at times, imperfectly—with CI stakeholder efforts to align practices with these other efforts. Given the potential for overlap and inconsistent guidance, CISA should explain how CI operators can best use this document vis-à-vis other resources. Creating baselines and recommendations is only one step in furthering cybersecurity, but achieving the goals set forth in the Control Systems Memorandum will require a focus on how such recommendations can be implemented and fit within an organization's big-picture cyber program.

V. THE COMMON BASELINE SHOULD FOCUS ON CI CONTROL SYSTEMS AND OPERATIONAL TECHNOLOGY—AS DIRECTED BY THE PRESIDENT.

A. The Control Systems Memorandum Tasks DHS with Developing Performance Goals for Control Systems.

The Control Systems Memorandum has a clear focus on CI control systems, and this intended scope should be carried through to the Controls List and Common Baseline, instead of

[41] *See generally* CSRIC Report.

[42] NIST SP 800-171 Rev. 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, NIST (Feb. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf.

these documents employing a wide-ranging approach. Within the Control Systems Memorandum, President Biden's intent was clear on this point. "Control Systems" is in the title of the Memorandum and the introduction references cybersecurity threats to "the systems that control and operate the critical infrastructure on which we all depend[.]"[43] The Memorandum section addressing CI cybersecurity performance goals discusses the need for "security controls for select critical infrastructure that is dependent on *control systems*" and tasks DHS with issuing "goals for *control systems* across critical infrastructure sectors."[44] Indeed, the Control Systems Memo refers to these goals as "cross-sector *control system* goals."[45] Accordingly, consistent with the President's directive as reflected in the Controls System Memorandum, the Common Baseline should limit its focus to goals for control systems.

B. The Common Baseline Should Be Focused on OT, Which Has Distinct Characteristics that Warrant Distinct Cybersecurity Approaches.

Consistent with focusing on control systems, the Common Baseline should be directed at OT systems rather than broadly encompass information technology ("IT") systems. Generally speaking, OT and IT systems can differ in ways that may have significant implications for their cybersecurity postures. OT systems include a wide array of systems and devices that interact with the physical environment. As NIST explains, OT is defined as:

> Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.[46]

[43] Control Systems Memorandum.

[44] *Id*. §§ 4, 4(b) (emphases added).

[45] *Id*. § 4(b) (emphasis added).

[46] *See* NIST SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, NIST at 101 (Dec. 2018), https://doi.org/10.6028/NIST.SP.800-37r2

In contrast, IT systems typically manage data and information, defined by NIST as "services, equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information[.]"[47]

Certainly, there is a growing consensus that IT and OT systems are converging—a trend that is being explored by the President's National Security Telecommunications Advisory Committee report that it is drafting on "IT/operational technology convergence" as part of its "Enhancing Internet Resilience in 2021 and Beyond" study.[48] But even still, OT and IT systems have varying characteristics that, in many cases, require distinct approaches. For example, OT systems include supervisory control and data acquisition systems, which are used to monitor oil and natural gas pipelines or rail systems, among other physical CI systems.[49] OT systems can also include distributed control systems that manage production systems in factories and processing facilities.[50] IT systems, which include email, customer billing, and other purely business functions, tend to prioritize data and information confidentiality. As NIST's recent draft *Guide to Operational Technology (OT) Security* explains, "OT have unique performance and reliability requirements and often use OSs and applications that may be considered

("NIST 800-37 Rev. 2")*; see also Glossary: operational technology*, Computer Security Resource Center, NIST, https://csrc.nist.gov/glossary/term/operational_technology (last visited August 3, 2022).

[47] *See* NIST SP 800-37 Rev. 2 at 100; *see also Glossary: information technology*, Computer Security Resource Center, NIST, https://csrc.nist.gov/glossary/term/information_technology (last visited August 3, 2022).

[48] President's National Security Telecommunications Advisory Committee (NSTAC) Meeting Summary, NSTAC at 7 (May 6, 2021), https://www.cisa.gov/sites/default/files/publications/May%202021%20NSTAC%20Meeting%20Summary_0.pdf.

[49] *See* NIST SP 800-82 Rev. 2 at 2-6.

[50] *See id*. at 2-10.

unconventional to typical IT personnel."[51]

These often different characteristics and functions of OT and IT systems can lead to variations in cybersecurity considerations. Diverse OT systems and their close interaction with physical processes can yield a different security posture than IT systems. While compromises to IT systems may lead to a loss of data or reputational harms to a company, a compromised OT system could result in harms to the physical world, such as breakdowns in transportation or factory accidents.[52] At the same time, threats to IT systems are dynamic because components are more fluid and intertwined than OT systems, which may be more static and have fewer avenues for attack.[53] NIST has also explained that IT systems tend to have standard communications protocols and networking practices, while OT systems typically use more varied communications protocols and complex networks that may require expert supervision.[54] In recognition of these varying attributes, NIST has developed distinct security guidance for OT and IT systems.[55] In addition to NIST, the Department of Energy's Office of Energy Efficiency and Renewable Energy has noted that security for OT is often weighed differently than IT, in terms of prioritizing the goals of availability, confidentiality, and integrity.[56]

Accordingly, because of the differences between OT and IT and in line with the Control

[51] Draft NIST SP 800-82 Rev. 3 at *xv*.

[52] *See* An Executive Guide to Cyber Security for Operational Technology, GE at 8 (2017), https://www.ge.com/fr/sites/www.ge.com.fr/files/an-executive-guide-to-cyber-security-for-operational-technology-whitepaper.pdf ("GE OT White Paper").

[53] *See id*. at 18-19.

[54] Draft NIST SP 800-82 Rev. 3 at 24-28.

[55] NIST SP 800-82 targets Industrial Control Systems and, in April 2022, NIST released a draft Revision 3 that would expand the scope of the document to all OT. *See generally* Draft NIST SP 800-82 Rev. 3.

[56] *Operational Technology Cybersecurity for Energy Systems*, Department of Energy, https://www.energy.gov/eere/femp/operational-technology-cybersecurity-energy-systems (last visited August 3, 2022).

Systems Memorandum, CISA should maintain a focus on OT systems rather than IT systems in the Common Baseline. However, to the extent the Common Baseline does impact IT systems, their reach should be limited to IT in operational environments, not *all* IT within an CI owner or operator's system.

C. CISA Should Reconsider the Scope of Some of Its Controls to More Properly Focus on OT.

Some of the guidance in the Draft Controls List is overly broad, reaching IT systems that may have characteristics necessitating a varied cybersecurity approach. As detailed below in Table 2, CISA should refine the scope of certain controls to focus on control systems and OT, and to the extent the CISA's work reaches IT, it should only reach IT in operational environments. These recommended revisions to the controls are in addition to the recommended revisions in Table 1 above, which are focused on ensuring the controls are not prescriptive.

Table 2

Control	Draft Text	Feedback
1.4	"Phishing resistant MFA should be implemented to reduce the risk of initial access and credential access attacks on. This control should be verified by the enrollment of all IT user accounts in MFA. For control systems assets, MFA should be enabled whenever possible, especially where remote access is being utilized, as well as all engineering workstations and HMIs."[57]	CISA should remove or caveat the recommendation to enroll "all" IT user accounts in MFA. Various IT systems address a myriad of functions, and it is not evident that all of them are sensitive enough to require MFA.
1.6	"An organization should maintain unique credentials for a single user across similar services on IT and OT, in order to reduce the risk of initial	The Common Baseline should not reach all IT systems. Controls that include all IT systems within their scope stretch beyond the Control Systems Memorandum and fail to consider nuanced differences between IT and

[57] Draft Controls List at 4.

Control	Draft Text	Feedback
	access on both IT and OT assets. This control should be measured by confirming that IT and OT assets require unique credentials in order to access an account."[58]	OT. CISA should make clear that this control is focused on IT in operational environments, and it should include the phrase "where appropriate."
5.1	"Owner/operators should patch all Known Exploited Vulnerabilities in all public facing systems to reduce the risk of defense evasion by threat actors. Asset owners should validate that the KEV's listed at Known Exploited Vulnerabilities Catalog | CISA are patched within the designated timeframe. When patching is not feasible, compensating controls should be applied and documented."[59]	As discussed in Table 1, patching decisions in OT systems are complex. In certain instances, patching could lead to greater harm, including impairing the functionality of an operational system. The Common Baseline should take these realities into account and include a discussion about vulnerability management that is tailored to OT. Further, requiring patching of *all* systems issues is overly broad. Vulnerabilities to some IT systems may not merit the resources to rapidly patch them or institute compensating controls; these decisions should be made at the organization level based on risk.
8.1	"Owners/operators should limit the connections between IT and OT to the greatest extent possible to reduce the risk of threat initial access via pivot from IT to OT. Organizations should verify that all OT/IT connections are logged and monitored for suspicious activity or unauthorized access."[60]	CISA should remove or caveat the recommendation that "all OT/IT connections" be monitored, or clarify the scope of the control. Resources for round-the-clock monitoring should be allocated according to risk.

VI. CONCLUSION

The Associations applaud CISA on its work to engage with industry on the Common Baseline, which can help organizations across sectors, of all varieties, implement effective cybersecurity practices to protect CI control systems. The Associations are pleased to be a

[58] *Id.*

[59] *Id*. at 12.

[60] *Id*. at 19.

resource on these issues and looks forward to collaboration to ensure that CISA's Common Baseline—including the Controls List—is effective, implementable by a range of organizations, and futureproof. To that end, the Associations and their members would be happy to meet with CISA as it finalizes the Common Baseline to answer questions and to provide further feedback.

Respectfully submitted,

/s/ Tom Power
Tom Power
Senior Vice President and
General Counsel

Tom Sawanobori
Senior Vice President and
Chief Technology Officer

CTIA – The Wireless Association
1400 16th Street, NW, Suite 600
Washington, DC 20036

/s/ Loretta Polk
Loretta Polk
Vice President and Deputy
General Counsel

NCTA – The Internet & Television Association
25 Massachusetts Avenue, NW – Suite 100
Washington, D.C. 20001

/s/ Paul Eisler
Paul Eisler
Senior Director,
Cybersecurity

USTelecom – The Broadband Association
601 New Jersey Avenue, NW, Suite 600
Washington, DC 20001

August 15, 2022