Comments from the Center for Internet Security in Response to the NIST Request for Information on "Developing a Framework To Improve Critical Infrastructure Cybersecurity"

The Center for Internet Security (CIS) is a 501(c)(3) nonprofit organization whose mission is to improve cyber security readiness and response in both the public and private sectors, and whose guiding principle is one of collaboration and partnership in order to collectively enhance our nation's cyber security posture. In that regard, CIS is well positioned and eager to assist in meeting the requirements of a cost-effective, cross-sector and consensus-based Cybersecurity Framework. These comments in response to the NIST RFI are intended to describe why CIS Security Benchmarks, and related CIS Benchmarks-based automatable security content, should be included as a foundational element of the Framework, and why such integration would likely aid in the effectiveness and applicability of the Framework as a cyber risk mitigation program across multiple critical infrastructure sectors.

CIS Security Benchmarks Provid Configuration Guidance for th Most Commonly Used Technologies

CIS Security Benchmarks are complete configuration security baselines covering many of the world's most widely used technologies. There are over 70 currently supported CIS Benchmarks spanning 14 technology groups (server operating systems (OSs), desktop OSs, databases, web servers, mobile devices, web browsers, etc.) CIS Benchmarks are available to the public at no cost as downloadable PDFs; they are available as automated, customizable resources in machine-readable formats for CIS Security Benchmarks members. Implementing all, or even many, of the security configuration recommendations within a CIS Benchmark will build into a system or application automated enforcement of an organization's configuration management policy or plan. Additionally, subsets of similar configuration recommendations within a CIS Benchmark are grouped to depict conformance with and implement other organizational policies/standards associated with the subject technology, such as identification and authentication, audit and accountability and access control. Each configuration recommendation is also written at the procedural level and includes, wherever feasible, automatable remediation and audit instructions for that particular configuration security control.

Further, many CIS Security Benchmarks are expressed in open standard schemas, including Extensible Configuration Checklist Description (XCCDF), the component specification for writing machine-readable benchmarks/checklists contained within the Security Content Automation Protocol (SCAP). CIS is also engaged in exploring additional opportunities to support the production and contribution of new Open Vulnerability and Assessment Language (OVAL) schemas and content for performing standards-based automated system checks based on CIS Benchmarks recommendation-specific XCCDF policy. Additionally, CIS has already communicated to NIST its intent to submit more CIS Benchmarks-derived configuration issues to be approved as new Common Configuration Enumerations (CCEs), identifiers that correlate security-related configuration issues across various security configuration guidance documents and automated assessment tools. All of these activities are geared toward increasing the availability o CIS's Benchmarks-based configuration recommendations in SCAP component specifications, with the ultimate goal of helping to expand the availability of vendor neutral security software product assessment and reporting capabilities.

CIS Benchmarks ar Voluntary, Consensus-Based an Internationally Recognized Best Practice Standards

CIS Security Benchmarks have always and continue to be the result of a voluntary, consensus-based review and development process, with participation open to security configuration experts within and across the private sector, government and academia. This consensus-built quality of CIS Benchmarks is the primary reason why they are considered authoritative sources for security configuration across both the private and public sectors and around the world. **CIS Benchmarks are referenced as industry best practice system hardening guidance in such wide-ranging standards and guidelines as the *Payment Card Industry Data Security Standar*d (PCI DSS), *NIST Special Publication 800-128: Guide for Security Focused Configuration Management of Information Systems* and the Center for Strategic and International Studies' (CSIS) *Critical Controls for Effective Cyber Defense*.** If built into the Cybersecurity Framework, the expectation is that the size of CIS Benchmark consensus teams would grow even further and include more security experts representing critical infrastructure entities, as they would have an additional incentive to contribute their specific expertise and operationally shaped knowledge to future CIS Benchmark development.

CIS Benchmarks not only result from the consensus efforts of voluntarily participating subject matter experts, but they are also voluntarily adopted by organizations of all types and sizes as the security baselines for their IT systems and assets. Hundreds of thousands of CIS Benchmarks resources are downloaded each year by individuals from entities across the globe and representing every economic sector, including energy, banking and finance, healthcare, telecommunications and transportation. These organizations adopt CIS Security Benchmarks as their own configuration security standards primarily because they know they are the result of consensus agreement of security experts who have a wide variety of organizational and industry experience, a deep knowledge of the platforms covered by the Benchmarks, and an understanding of how the Benchmarks can meet both security and operational needs. Additionally, 30% of CIS Security Benchmarks enterprise members are located outside the U.S., primarily in Canada, Australia, the United Kingdom and other European nations. Such international membership representation is further testament to the recognition and acceptance of CIS Security Benchmarks as international standards.

We Can't Improve What We Can't Measure: Additional Customization of CIS Benchmarks is Helping Organizations Better Meet their Security Needs

The CIS Benchmark development process was essentially revolutionized in 2012 through the launch of a new collaboration platform and process that facilitates improved consensus building and near simultaneous generation of prose-based Benchmark security configuration recommendations and corresponding artifact expressions, providing the basis for standard, machine-readable XML content. The next goal for this still evolving platform, by no later than end of calendar year 2013, is to offer the tool to CIS Benchmarks members as a new security resource. This would provide those members a centralized, intuitive and easy to use mechanism for customizing recommendations within an existing CIS Benchmark so that recommended configuration settings can be adjusted to meet the specific security requirements of each adopting organization. Such customization capabilities would enable substantial flexibility for sector-specific operational environments that may need to weigh system/data availability higher than confidentiality, while still ensuring a fundamental level of security due diligence.

As previously noted, CIS will continue its efforts to express, and seek additional resource opportunities to support the expression of, more of its Benchmarks in SCAP-compliant, automatable content. CIS has also taken initial steps in leveraging another SCAP component schema, the Common Configuration Scoring System (CCSS), to prioritize Benchmark recommendations according to their CCSS scores (which are based on exploitability and security impact) assigned to each of a system's or application's configurable states. CIS has already developed "beta" versions of Benchmarks in PDF format that include only Benchmark recommendations corresponding to "High" (7 - 10) CCSS scored configuration issues. A longer-term goal, dependent on the availability and timing of necessary resources, is to also integrate CCSS scores into the CIS collaboration platform. This would provide CIS Security Benchmarks members the ability to leverage a central resource for not only customizing their IT asset-specific textual policies/standards and associated XML policy and check content, but also the capability to prioritize configuration controls so that they can address the most critical configuration issues first.

The more CIS Benchmarks that are produced in SCAP component, automatable schemas such as XCCDF, OVAL and CCEs, the more cost-effective, repeatable and measurable they will become for those that leverage them. The SCAP specification and component standards are intended to provide consistent, repeatable methods for mitigating and managing system vulnerabilities and measuring security effectiveness and compliance. Increasing the amount and availability of SCAP content based on industry-accepted security standards such as CIS Benchmarks will expand and enhance capabilities for performing consistent and comparable assessments and reporting across organizations and even infrastructure sectors. SCAP is also meant to foster vendor product neutrality and thus engender a more competitive and lower cost market for such security assessment tools. And such products often provide dashboard-type reporting capabilities for measuring and monitoring security and compliance improvement over time.

CIS Benchmarks are Helping Improve Security Across Broa Range of Sectors

As aforementioned, CIS Security Benchmarks are accessed and used by enterprises representing a range of industries and critical infrastructure sectors. In fact, about 35% of the thousands of CIS Benchmarks resource downloaders identify their organizations as either belonging to the energy, banking and finance, healthcare, telecommunications or transportation sectors (based on resource download statistics measured from February thru June 2012). And over 25% of current CIS Security Benchmarks members represent those same sectors. These figures make clear that CIS Benchmarks and associated automated assessment resources are already being utilized by critical infrastructure owner/operators to improve the resilience of their IT systems and assets.

The broad technology coverage of CIS Benchmarks facilitates their applicability to many critical infrastructure sector-specific systems, which often are built upon common operating systems and/or are integrated with other traditional business applications. Additionally, CIS Benchmarks are frequently leveraged by consulting/auditing firms as an important component of performing compliance audits particular to critical infrastructure sectors, such as requirements related to system/data security as part of HIPAA Security Rule compliance assessments for healthcare sector entities and SOX and GLBA compliance audits for financial services sector companies.

There are CIS Benchmarks for an already extensive and growing number of technologies and varieties of platforms within technology groups. For example, for server and desktop operating systems there are CIS Benchmarks for Microsoft, Linux (Red Hat, SUSE Linux and Debian) and

UNIX (Apple OSX, IBM AIX, Oracle Solaris and HP-UX) platforms. For mobile devices, there are Benchmarks for both Google and Apple devices, with additional product coverage planned for the near-term. (To browse all 70-plus currently supported CIS Benchmarks, please visit: https://benchmarks.cisecurity.org/downloads/browse.) Such broad technology and brand coverage does not force or even incentivize a critical infrastructure entity or any type of organization to have to choose certain software vendor systems or applications in order to secure them according to CIS Benchmarks. Further, as more CIS Benchmarks are expressed in SCAP-compliant open standards, the more choice an organization will have in vendor security assessment products, as there are a growing number of such tools that can assess system configurations utilizing such content. Such increasing solution choice, and resulting market competition and price reduction, is really what open standards are all about.

Working Together, We Can Improve Our Nation's Cyber Readiness an Response

For almost thirteen years, CIS has nurtured a trusted environment where experts have voluntarily come together to work toward a common goal: improving the security of our collective IT systems and assets. CIS will continue to endeavor to not only be a leader in producing consensus-based configuration security standards but also in seeking out additional opportunities to express its guidance in SCAP-based, automatable formats. CIS is also engaged and actively participating in the current efforts to move SCAP-related schemas into the Internet Engineering Task Force (IETF), which should further increase contribution to and adoption of those technologies by private sector and international entities.