TO: Ms. Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

DATE: February 23, 2016

SUBJECT: Views on the Framework for Improving Critical Infrastructure Cybersecurity

---

The Chertoff Group (TCG) appreciates the opportunity to comment on the National Institute of Standards & Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (the "Framework"). TCG works with clients across a number of sectors to help them assess, manage and monitor their security programs. We also work with the providers of security products, services and solutions to grow their enterprise through business strategy and mergers and acquisitions services.

The targeting of organizations across multiple industry sectors by malicious actors is not new, but the proliferation of malicious actor tactics, techniques and procedures, combined with complex and aging information technology (IT) applications and infrastructure, leaves organizations increasingly vulnerable to attack. Based on our cybersecurity risk management experience, we believe that elimination of cyber risks is futile. Nevertheless, it is both possible and essential to build a cybersecurity program that provides an organization with reasonable, risk-based security controls to secure sensitive technology assets notwithstanding these risks. The NIST Framework is a valuable resource for organizations building and managing cybersecurity programs.

Our security professionals have had the opportunity to reference and apply the Framework for our cybersecurity engagements across multiple critical infrastructure sectors. Organizations and associations have consulted with us to better understand their cybersecurity maturity and to improve their overall cybersecurity posture and profile. The NIST Framework is an important tool that helps us converse with all manner of clients, and their diverse personnel, on managing cyber risk. For example, during an engagement with a Fortune100 company we leveraged the Framework to help validate the company's cybersecurity roadmap. Incorporating the Framework into our Chertoff Group Risk Management methodology provided an effective way to describe and discuss capabilities across business and regional units to both technical and non-technical personnel.

Through our review and use of the Framework, we have identified several topics NIST may wish to consider addressing in the next iteration of the Framework:

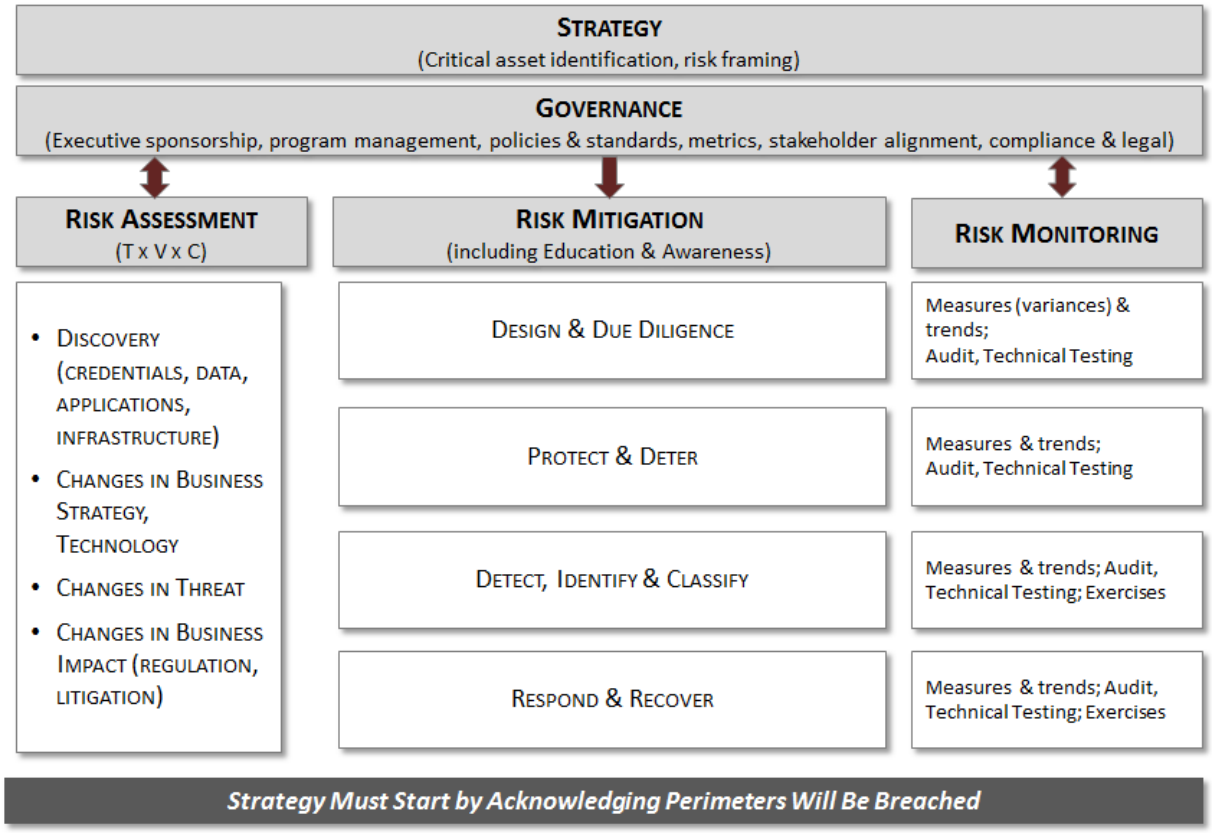
Strong authentication should be expressly referenced: Exploitation of weak or stolen credentials continues to grow as a key attack vector, which is why stronger authentication, in particular multifactor authentication, is recommended for organizations to secure their networks and critical information assets. And yet the Framework makes no reference to consideration of strong authentication. As

indicated in multiple authoritative reports and guidance, including DHS' US-CERT reporting and Verizon's 2015 Data Breach Investigations Report, use of multifactor authentication for remote access is considered as an important risk reduction measure. During our TCG cybersecurity engagements, our security teams have observed that strong multifactor authentication, especially for remote access, is being adopted across sectors. At a minimum, we recommend that in the next iteration of the Cybersecurity Framework, NIST include a reference to the use of strong authentication across relevant access control subcategories.

Privileged account management should be expressly called out in the Access Control category: The compromise of privileged user credentials is a common aspect of breaches across a number of sectors and, in our understanding, this dynamic explains why the Center for Internet Security Critical Security Controls (CSC) for Effective Cyber Defense were reordered (in Version 6.0, the most recent version released last fall) such that controlled use of administrative privilege is a higher priority (up from #12 to #5). In other words, malicious actors have repeatedly obtained privileged user credentials and used those credentials to stand in the shoes of the legitimate user. And yet, the only explicit reference to privileged user-related controls appears in the Training category. The Framework should draw express focus to security of privileged user credentials.

Response-oriented engineering should be articulated in the Framework: Response efforts can be significantly complicated if certain capabilities are not implemented pre-event. For example, the U.S. Department of Justice April 2015 Best Practices for Victim Response and Reporting guidance highlights the importance of proper logging procedures as a foundation for effective response. Retention periods and security around logs can be critical factors in a response effort. TCG believes that the concept of "Response-oriented Engineering" (RoE) should be included within the Framework's Protect, Response and Recover functional and subcategory areas. RoE, or the development of systems, networks and applications built by design with the ability to effectively support incident response, is a growing area of interest by organizations looking to respond more successfully to cyber incidents. For example, while the Framework does include references to audit and logging controls, NIST should consider more explicitly linking implementation of logging to response and recovery.

Guidance on implementation and effectiveness measures should be provided: NIST Special Publication (SP) 800-39, on managing information security risk, articulates a continuous process of assessing, responding to and monitoring risk, and yet the Framework contains little guidance on how each category may be monitored for implementation and effectiveness. We use the model below and offer it as an example of how NIST 800-39 and the Framework can be aligned.



In other words, as SP 800-39 notes, trust in the security of information systems is a function of both security functionality and assurance. We understand that the Framework is intended for use by a wide variety of organizations, and we would indeed caution against overly prescriptive guidance on risk monitoring measures. That said, we recommend NIST include guidance, perhaps at a high level, on how organizations might consider measuring implementation and effectiveness of specific categories.

Descriptions of Subcategories: The descriptions of the Functions and Categories included within the Framework Core documentation are helpful in providing general indicators of which security control area is covered. In addition, the Informative References are useful in crosswalking Framework subcategories with other, longstanding control regimes. However, the subcategory descriptions leave ambiguity in places, for example, whether a vulnerability management plan contemplated in PR.IP-12 applies to applications as well as operating systems. In the next Framework iteration, TCG recommends additional language be included to describe the subcategories so that users better understand what each subcategory addresses.

Informative Reference crosswalks should be more detailed: One critical aspect of the Framework is the crosswalk to other Informative References, and yet this crosswalk is only partially complete. For example, the CSC crosswalk exists only at the control rather than subcontrol level. As a result, particularly meaningful CSC subcontrols, such as the one referring to two-factor-authentication-for-remote access, are absent from the Framework's Informative References section. Moreover, in certain cases, entire CSC control categories are absent from the crosswalk – for example CSCs related to

application software security; controls on network ports, protocols and services; and boundary defense and penetration testing.

Thank you for the opportunity to provide these comments. TCG welcomes any questions you may have regarding these comments.

For further information please contact:
Chris Duvall
The Chertoff Group
202-552-5280
chris.duvall@chertoffgroup.com