From:	Lumeta Corporation, Reginald P. Best
Proposal:	1550 (RIN 7100--AE-61) (Ver 1)- Enhanced Cyber Risk Management Standards
Subject:	Enhanced Cyber Risk Management Standards

Comments:

Reginald P. Best
President & Chief Product Officer
Lumeta Corporation
rbest@lumeta.com
www. umeta.com
732 357 3529

This public comment pertains generally to questions 26, 27 and 28 of the joint advance notice of proposed rulemaking for Enhanced Cyber Risk Management Standards – subsequently referred to in this comment as the "proposed rulemaking".

Lumeta Corporation has over the past decade provided network-based cyber situational awareness analytics tools and services to seven (7) of those largest ($50B in assets) financial institutions that may be covered by the proposed rulemaking. These comments represent a summary of our experiences with these clients.

26. How do covered entities currently evaluate their situational awareness capabilities? What factors should the agencies consider essential in considering a covered entity's situational awareness capabilities?

In our experience covered entities have limited tools or processes to authoritatively evaluate their situational awareness. There is a false sense of security that organizations have that they know and understand what is happening on their networks. Despite investment in multiple tools at various places in the enterprise "security stack" which typically span network change management and access control, endpoint detection and response, host vulnerability assessment, simulation and "what if" analysis, SIEM, GRC, etc., the very basic understanding of what constitutes the network, how it changes in real-time, what the infrastructure comprises (approved versus rogue), what the authoritative topology of the network and network edge is, remains elusive and is often an afterthought.

Sadly, the attack surface of the covered entity is not well understood as a result and all the other security stack components further up the food chain become less effective without this fundamental understanding. Simply put, covered entities miss the infrastructure that they don't know about because they forget to document it (human error), aren't uniformly aware of it (information silos within departments) nor are they hunting for network state changes constantly to validate they have an accurate understanding. It is usual in the Lumeta experience to find scores or hundreds of operational networks, hosting thousands or tens of thousands of devices which are essentially un-managed, because the understanding of the underlying network is inconsistently accounted for and only at infrequent points in time via an incomplete scanning/discovery or perhaps manual activity.

The agencies should consider as a cornerstone of the proposed rulemaking

whether the covered entity has an automated and authoritative network indexing capability supplying holistic network situational awareness metadata which can be used by cyber security stack elements that are further up the security analysis and protection food chain.

For more information:
http ://www. lumeta .com/wp-content/uploads/2016/10/FFIEC-OCC-Cybersecurity-with-Lumeta-ESI-Solution-Brief.pdf

27. What other factors should be included within the incident response, cyber resilience and situational awareness category?

The ability to provide both cyber resilience and accurate incident response are hampered by misunderstandings of a covered entity's network infrastructure elements, topology and edge. It is also hampered by misunderstanding the L3 routed paths that exist between internal network enclaves and/or between certain enclaves and the public Internet (e.g. network segmentation and routing rules). All of these are prone to human error, especially in large networks as infrastructure elements or configurations change. Malicious actors are constantly hunting for these kind of erroneous changes which they can take advantage of to achieve a beach head for their activity. Covered entities would be advised to constantly hunt for these kinds of weaknesses in an automated fashion in order to find and remediate them before the malicious actors can take advantage. Further, given the increasing use of virtualized software network functions, public IAAS cloud infrastructure and software defined networking it is increasing necessary for all network segmentation and routed path analysis to be considered a real-time need. It is quite possible for network situational awareness to be changed minute by minute in today's increasingly dynamic, software driven and virtualized networking infrastructures.

28. What additional requirements should the agencies consider to improve the resilience or situational awareness of a covered entity or the ability for a covered entity to respond to a cyber-attack?

The proposed rulemaking should consider over some reasonable time horizon that the real time detection of core network infrastructure security faults be used to feed enterprise-wide behavior analysis systems and orchestrate faster, immediate remediation of certain critical fault conditions. For example, if a subnetwork is designated by a covered entity to be "core", and a new, unexpected forwarding device or routed path to an unexpected destination (such as the Internet) appears, this may require an semi-automated or fully automated remediation response by the network infrastructure. Such capabilities are becoming possible via multivendor integration scenarios.