Board: Docket No. R-1550 and RIN 7100-AE-61 (via regs.comments@federalreserve.gov)
OCC: Docket ID OCC-2016-0016 (via regs.comments@occ.treas.gov)
FDIC: RIN 3064-AE45 (via comments@fdic.gov)

February 17, 2017

Microsoft Corporation's Comments on Joint Advance Notice of Proposed Rulemaking, Enhanced Cyber Risk Management Standards

I. Introduction and Executive Summary

Microsoft submits these comments in response to the federal banking agencies' joint advance notice of proposed rulemaking ("ANPR") regarding enhanced cyber risk management standards (the "proposed standards").[1] Microsoft is a major provider of technology products and services to the financial services industry, including the provision of cloud computing services that are an important and growing part of how the industry uses technology today.[2] The ANPR and the proposed standards represent a substantial undertaking that will have significant consequences not only for the financial services industry but also for third-parties like Microsoft that provide services to covered entities within the industry and that may therefore need to take account of the standards once finally issued.

The ANPR recognizes the evolving relationship between systemic risk in the financial services sector and the digital transformation taking place across the industry. Traditional concerns about criticality, interconnectedness, and contagion remain extremely relevant to financial institutions, their customers and their regulators. Yet the means of assessing and mitigating these risks are changing rapidly as the underlying technology evolves. These dramatic changes can challenge today's common assumptions.

For example, traditional on-premise computer networks that host sector-critical systems may actually present a comparatively high level of risk and low level of performance when compared with broadly-accredited cloud services. This is because best-in-class security, infrastructure redundancy, data replication, and low latency are typically difficult for individual institutions to obtain and manage within a reasonable cost structure in their on-premise solutions. In contrast, leading cloud services can provide sophisticated approaches to security at Internet scale and leverage highly-redundant infrastructure with data replication on a distributed basis,

[1] See Enhanced Cyber Risk Management Standards, 81 Fed. Reg. 74,315 (Oct. 26, 2016). As used herein, the "federal banking agencies" refers to the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation.

[2] Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

(continued...)

and with comparatively low latency, enabling operations that are both more secure and efficient. This new reality upends long-held notions that on-premise systems are more manageable and secure than are cloud-based systems. Today, many leading experts agree that cloud-based services provide controllability and scalability that individual financial institutions generally cannot achieve in their on-premises systems given their limited security capabilities and capacities.[3]

Against this background, Microsoft's comments are intended to address the relationship between systemic risk and technology, and to suggest certain respects in which the proposed standards can be appropriately shaped to allow technology to be most effectively utilized by financial institutions. Specifically, Microsoft's comments address three areas: (1) the overall approach to applying the proposed standards to sector-critical systems and covered services; (2) certain other issues raised in the ANPR, namely, the approach to be used by the federal banking agencies in implementing the proposed standards, methodologies potentially to be used for quantifying cyber risk and resilience in the context of cloud and other online services; and (3) the role of cloud services in mitigating low probability, high impact events that might compromise systemic functionality (i.e., black swan scenarios).

With respect to the ANPR's overall approach to subjecting sector-critical systems and covered services to the proposed standards, Microsoft recommends that:

- The proposed standards expressly recognize that covered entities may use third-party service providers to support sector-critical systems, and the standards be appropriately tailored in their application to such service providers.

- Identification of covered services and sector-critical systems be based on whether those services and systems perform functions that are truly critical within the financial services industry, and sector-critical standards be applied in a manner that recognizes the inherent capabilities of the underlying technologies.

Additionally, with respect to certain other issues raised in the ANPR, Microsoft recommends that:

- The proposed standards be implemented through the first approach identified in the ANPR, namely, by proposing the standards as a combination of a regulatory requirement for covered entities to maintain a risk management framework for cyber risks, along with a policy statement or guidance that describes minimum expectations for such a framework.

[3] See, e.g., Toward New Possibilities in Threat Management, PWC, available at http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/assets/gsiss-report-cybersecurity-privacy-possibilities.pdf (observing that because "traditional on-premise systems are often constrained by inadequate storage capacity, processing power and scalability" those limitations can "impede cybersecurity teams' ability to view and analyze data across their enterprise, restrict search efforts and increase the volume of false positives.").

- The FFIEC Cybersecurity Assessment Tool could be an appropriate measurement instrument for quantifying cyber risk, subject to some improvements in the Tool's risk and readiness assessment methodologies.

- The proposed standards recognize that, in the context of cloud and other online services, service provider commitments regarding service availability and downtime can provide covered entities with assurance concerning service resilience.

Finally, with respect to mitigation strategies to address black swan scenarios, Microsoft recommends that the agencies consider the significant security and resilience advantages that cloud services can offer in relation to managing and responding to constantly evolving cyber risks, ultimately making black swan events less likely to occur and more manageable if they should occur.

Part II of these comments provides a brief background regarding Microsoft's perspective on the proposed standards as both a major cloud services provider and an organization with deep experience with cybersecurity issues. Parts III-V set forth Microsoft's comments on the ANPR's overall approach to the proposed standards, certain other issues raised in the ANPR, and mitigation strategies for black swan scenarios.

II. Microsoft's Perspective on the Proposed Standards

Financial institutions as well as other businesses increasingly leverage cloud services that run on infrastructure owned and operated by third parties such as Microsoft. The use of such services can improve an institution's cybersecurity posture by drawing on the resources of the service provider to supplement and enhance an institution's own capabilities. For example, a cloud service provider ("CSP") may offer infrastructure capabilities that are cost-prohibitive for many institutions to establish in their own networks. Also, cloud service technologies rapidly integrate lessons learned from cybersecurity attacks and technical challenges in other environments, thus increasing the protections provided to the industry and mitigating classes of attacks.

Additionally, Microsoft is a leader in developing and implementing strong cybersecurity practices. As a global security advocate, Microsoft has made public its Security Development Lifecycle—now incorporated in an international standard on secure software development, ISO/IEC 27034-1—to provide a principled approach to building secure, enterprise-grade software.[4] This has enabled developers to build more secure software and address security compliance requirements while reducing development costs. Microsoft extends secure frameworks and practices into its cloud services operations as well, delivering an end-to-end vision for cloud-based security. Microsoft also works proactively to protect people and businesses from a broad range of cybercrime threats, including botnets and globally-distributed cybercrime networks. For example, Microsoft has established a Digital Crimes Unit composed of an international team of attorneys, investigators, data scientists, engineers, analysts and

[4] See Microsoft, Security Development Lifecycle, available at https://www.microsoft.com/en-us/sdl/.

(continued…)

business professionals based in 30 countries that work together in the ongoing fight against digital crimes.[5]

Microsoft fully concurs with the agencies that cybersecurity is rooted in risk management.[6] Effective cybersecurity programs focus on practices and controls that organizations can tailor in the face of their particular risk profiles and a shifting threat landscape. Organizations must dynamically recalibrate their approaches, based on the information available and the security solutions that work best within their individual environment. The speed with which security threats can change today requires an unprecedented agility from organizations. Thus, for example, where a particular technical approach is not feasible for an organization's architecture, it needs to be able to implement alternative reasonable solutions to mitigate security risks. Flexibility and adaptability are the hallmarks of robust cybersecurity management programs. With this is mind, it is critically important that regulators define what they want to achieve (i.e., outcomes), without being technically prescriptive about how that outcome is achieved.

III. Approach of the Proposed Standards

A. Application to Third Party Service Providers

Microsoft has two primary concerns in relation to the application of the proposed standards to third-party service providers. First and foremost, Microsoft seeks to maintain an open and competitive marketplace in which entities whose operations include sector-critical systems can continue to rely upon best-in-class third-party products and services in connection with those systems. The introduction of new standards can lead covered entities to develop in-house technology solutions and new compliance programs that divert resources away from actual cybersecurity activities and towards compliance activities. The end result can be a patchwork of compliance-centric implementations that do not offer security protections comparable to third-party technologies. Covered entities may under-resource important capabilities and capacities to assess the threat landscape, develop and actively manage their network protections, and generally keep pace with threats.

Additionally, Microsoft seeks to ensure maintenance of the traditional regulatory model in which organizations that choose to outsource activities retain ultimate responsibility for adherence to regulatory obligations. Both Microsoft and its customers have made significant investments in this area to ensure that customers—and their regulators—have the information they need to make appropriate determinations about outsourcing and to address regulatory requirements.

[5] See Microsoft, Digital Crimes Unit Fact Sheet, available at http://news.microsoft.com/download/presskits/DCU/docs/dcuFS_160115.pdf.

[6] See, e.g., Enhanced Cyber Risk Management Standards, 81 Fed. Reg. 74,320 (Oct. 26, 2016) ("The enhanced standards would emphasize the need for covered entities to demonstrate effective cyber risk governance" and "continuously monitor and manage their cyber risk within the risk appetite and tolerance levels approved by their boards of directors" among other requirements).

To ensure that covered entities have maximum access to best-in-class technology products and services, Microsoft recommends that the proposed standards expressly recognize that covered entities may utilize third-party service providers to support sector-critical systems. Without this crucial clarification, the proposed standards could inadvertently discourage covered entities from utilizing third-party service providers in sector-critical scenarios. Clear recognition that third parties can be used to support sector-critical systems will ensure that covered entities are appropriately empowered to address their technology needs through leading-edge solutions.

It appears that the agencies concur with this recommendation. For example, questions four and five in the ANPR contemplate both direct and indirect application of the proposed standards to third parties, although these questions do not squarely address the nexus between third-party outsourcing and sector-critical systems.[7] The agencies should clarify this point through specifically acknowledging the permissibility of outsourcing sector-critical systems.

With regard to how the proposed standards may be applied in third-party relationships, Microsoft recommends that the agencies develop an approach that is consistent with traditional regulatory models in which the covered entity retains ultimate responsibility for adherence to regulatory requirements in outsourcing scenarios. For example, where a covered entity uses a cloud service to provide the platform for a sector-critical system, the covered entity would need to take the system's sector-critical designation into account in establishing the configuration of the cloud services, such as by enabling encryption for data at rest and/or in transit. At the same time, because other elements of the underlying cloud service (e.g., data centers) are utilized by a broad array of organizations that may not operate sector critical systems, it would be impractical to require the CSP to support sector-critical standards for all elements it provides. This is precisely why CSPs—even in the context of a standardized online service—offer customers the ability to elect additional features that can further strengthen the security of their individual deployments.[8]

Moreover, it is important that the proposed standards be appropriately tailored in their application to CSPs as well as other types of third-party services providers.[9] Microsoft

[7] See Enhanced Cyber Risk Management Standards, 81 Fed. Reg. 74,319 (Oct. 26, 2016).

[8] For example, Microsoft offers services that enable enterprise cloud users to assess and reconfigure their cloud deployments based on our recommendations to enhance security. Microsoft offers these services on an elective basis, meaning that customers must choose to activate them and accept related costs. For regulated customers, these services can support compliance activities against a broad range of baselines.

[9] While recognizing that the proposed standards may be applied to third-party providers, it also is Microsoft's understanding that the new standards as proposed would be applied to service providers through existing regulatory processes and will not involve the creation of new regulatory processes. For example, a company that provides covered services and that is examined by a federal banking agency pursuant to the Federal Financial Institutions Examination Council's ("FFIEC") supervisory program for technology service providers ("TSPs") presumably would be examined for compliance with the proposed standards as adopted. Similarly, a service provider that is subject to an ad hoc examination by one of the federal (continued...)

appreciates that the federal banking agencies have recognized the need for appropriate tailoring in the ANPR by indicating that, in the case of service providers, "enterprise-wide" standards are to be applied only to the portions of a provider's services related to or affecting the provider's performance of services for a covered entity.[10] The ANPR likewise appropriately recognizes that, "depending on the size and structure of the [service provider] organization and the relative size of the unit providing services to a depository institution, its subsidiaries or affiliates, it may be appropriate for some functions to be performed by business line executive management instead of the board of directors or a board committee of the organization."[11] Microsoft supports this sort of tailored approach to the application of the proposed standards in scenarios involving cloud and other third-party service providers.

B. Identification of Sector-Critical Systems

The agencies put forward several questions stemming from the fundamental inquiry of how sector-critical systems should be identified, with the ANPR outlining both quantitative and qualitative factors that may be considered. As a starting point, Microsoft concurs with the agencies approach to including qualitative factors as potential means of identifying sector-critical systems.[12] Qualitative factors can enable a more nuanced view into how the financial system operates. Likewise, qualitative factors allow for an interpretative approach to regulatory policy, which is appropriate because technology continues to evolve rapidly.

In regard to the qualitative assessment measures under consideration, such as whether a system provides a key functionality for which alternatives are limited or nonexistent, it is crucial that agencies deliberately take a narrow approach in the further development and application of these tests.[13] In particular, any qualitative assessment should recognize that one part of a system may be sector-critical, without requiring that all related systems be treated as sector-critical. Given the variety of technology systems that may exist within any individual covered entity today, it would be ineffective and inefficient to treat all connected systems as sector-critical simply because some part of the entity is deemed sector-critical.

For example, in an institution where financial systems relying on cloud services are deemed sector-critical, other non-critical systems on the same infrastructure should not be deemed sector-critical as well. There may be significant management and control differences between these services within the various services provided by the CSP. Such an overly inclusive approach could dilute the focus of supervisory activities, as well as unnecessarily increase requirements for covered entities and their third-party providers.

banking agencies in connection with its provision of cybersecurity services to a regulated institution also would be reviewed for compliance with the proposed standards as adopted.

[10] See Enhanced Cyber Risk Management Standards, 81 Fed. Reg. 74,320 n.14 (Oct. 26, 2016).

[11] Id.

[12] Id. at 74,319.

[13] Id.

In this regard, whatever specific measures or tests the agencies develop, the agencies should identify sector-critical systems based on the specific functions that are critical within the financial services industry—and then apply the sector-critical standards to the particular systems that support those functions. Accordingly, Microsoft further recommends that size alone should not be a driver of whether a system is sector-critical. Application of a size-based model or a model focused on consolidation of activity on a certain network or platform would fail to recognize that the technologies used by covered entities may have been demonstrated to entail either greater or lower risk, depending on their particular capabilities and the functions for which they are being used within an institution or the larger financial ecosystem. For example, a size-based approach does not take into account the resiliency and threat protection built into the technical systems that can protect against cyber threats.

Pervasiveness likewise should not be the main driver of whether a system is sector-critical. First, not all systems offered by broadly-used providers are functionally sector-critical. For example, certain email platforms are pervasive in the financial industry and are likely used to some extent by the majority of covered entities. But if email systems fail, such failure is not likely to lead to a systemic cybersecurity risk or harm. By contrast, to the extent that core banking functions—such as customer transaction processing and customer account-record maintenance—are moved to a particular cloud platform, it obviously is important that appropriate compliance steps be taken by the entity outsourcing its activities, so as to ensure that the CSP adheres to appropriate practices.

In short, standards that identify sector-critical systems based on the functions that are critical within the financial services industry will not only advance cybersecurity in an appropriately targeted manner but will also provide important clarity as to the proper treatment of individual systems both to covered entities and to service providers that help run such entities' supporting technologies.

IV. **Additional Issues Raised in the ANPR**

A. Implementation of Standards

Standards are important. But standards compliance alone does not equal security. Threats move much faster than the glacial pace of standards development. This is precisely why Microsoft has innovated using its SDL expertise to create the Operational Security Assurance framework that rapidly integrates threat intelligence into security science to mitigate potential attacks.[14] It is from this perspective that Microsoft strongly urges that, in implementing the proposed standards, the federal banking agencies not issue highly prescriptive regulatory standards, which could hinder the ability of covered entities and their service providers to manage and respond to new and evolving cyber threats.

Effective cybersecurity programs focus on practices and controls that organizations can tailor in the face of their particular risk profiles and a shifting threat landscape. Organizations must dynamically recalibrate their approaches, based on the information currently available to

[14] Microsoft Trustworthy Computing, Operational Security for Online Services Overview, Oct. 21, 2013, available at https://www.microsoft.com/en-us/download/confirmation.aspx?id=40872.

them and the security solutions that will work best within their individual environments at the time. Thus, for example, where a particular technical approach is not feasible for an organization's current architecture, it needs to be able to implement reasonable, alternative solutions to mitigate the security risks it faces. Flexibility and adaptability are the hallmarks of robust cybersecurity management programs.

Federal standards bodies have recognized the need for flexibility and adaptability in cybersecurity risk management. Thus, for example, the National Institute of Standards and Technology Cybersecurity Framework (the "NIST Framework") expressly states that it is "not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure" because "[o]rganizations will continue to have unique risks—different threats, different vulnerabilities, different risk tolerances—and how they implement the practices in the Framework will vary."[15] Moreover, the NIST Framework's maturity model recognizes that an "[a]daptive" approach to cybersecurity risk management is the most sophisticated.[16]

Risk-based approaches are familiar in the financial services regulatory context as well. Thus, the FFIEC Cybersecurity Assessment Tool is based largely on the NIST Framework, to assist organizations in determining the relationship between their inherent risk and their readiness to address that risk.[17] And the FFIEC IT examination process likewise is based on a risk-based approach to the ongoing supervision of technology service providers.[18] This includes a recognition that while all institutions "should implement appropriate controls," "[t]he level at which controls are implemented should depend on the institution's size, complexity, and risk profile."[19]

For these reasons, Microsoft believes the best approach to implementation here is the first approach identified in the ANPR—namely, proposing the standards as a combination of a regulatory requirement for covered entities to maintain a risk management framework for cyber risks, along with a policy statement or guidance that describes minimum expectations for the framework, such as policies, procedures, and practices commensurate with the inherent cyber risk level of the covered entity. Microsoft recommends that the federal banking agencies adopt this approach to implement the proposed standards.

[15] See National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Feb. 12, 2014, at 2, available at https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[16] Id. at 9-11.

[17] See Federal Financial Institutions Examination Council, Cybersecurity Assessment Tool, June 2015, available at https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_June_2015_PDF2.pdf.

[18] See, e.g., Federal Financial Institutions Examination Council, Information Technology Examination Handbook, Information Security, September 2016, available at http://ithandbook.ffiec.gov/media/216407/informationsecurity2016booklet.pdf.

[19] Id. at 13.

(continued...)

B. Quantifying Cyber Risk

Microsoft recognizes that developing methodologies to measure cyber risk, particularly as it relates to the interdependencies of systems, is a complicated and challenging exercise. In Microsoft's experience, the best approach within the scope of current capabilities is to make available, and encourage the use of, commonly-accepted risk assessment frameworks.

In this regard, Microsoft supports the use of the FFIEC Cybersecurity Assessment Tool ("Tool") as a measurement instrument. Indeed, Microsoft submitted comments in support of the Tool. As those comments indicate, Microsoft views the Tool as an important and significant step forward in the process of improving cybersecurity in the financial services sector. The Tool also reinforces many cybersecurity risk management practices that Microsoft and other leading technology companies have supported, such as the importance of secure development practices and the replacement of systems that have reached end-of-life with modern, more secure systems.[20] Moreover, the Tool promotes regulatory harmonization by mapping to the NIST Framework, which is a widely-recognized reference point internationally as well as domestically for critical infrastructure cybersecurity.[21]

At the same time, Microsoft does continue to have certain concerns about the Tool's treatment of cloud services. For example, the Tool's quantitative approach focuses on factors such as the number of CSPs used by an organization and on binary deployment considerations such as whether an organization uses public or private cloud, or leverages domestic or overseas data centers.[22] Rather than focusing on such blunt factors and considerations, however, Microsoft believes that cyber security goals may be better served by focusing on the provider's compliance and risk management posture, including whether the CSP meets certain national and international standards for cybersecurity and privacy. In addition, the Tool states that an absence of cloud services presents no inherent risk when weighed against the option of using cloud services. However, this is only true in instances in which the on-premise system has been designed, built, operated and maintained to meet the strict requirements for integrity, security, availability, privacy and confidentiality that many cloud services are designed to meet. Instead, Microsoft recommends that risk measurement tools take into account a CSP's ability to demonstrate it can deliver a trusted cloud that meets well-recognized security standards.

C. Addressing Recovery Time Objectives and Service Resilience in Cloud and Other Online Services

The agencies raise several questions related to the determination of appropriate Recovery Time Objectives ("RTOs"). RTOs certainly are one relevant line of inquiry in connection with resilience planning. However, Microsoft would note that dialogue between CSPs and regulated financial institutions typically focuses primarily on specific commitments pertaining to service

[20] See Federal Financial Institutions Examination Council, Cybersecurity Assessment Tool, June 2015, at 12, available at https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_June_2015_PDF2.pdf.

[21] Id. at Appendix B.

[22] Id. at 13.

availability and downtime that are backed up by express contractual guarantees in Service Level Agreements ("SLAs"). This focus provides fundamental advantages to a financial institution, as it contractually obligates the CSP to deliver highly available services with truly minimal disruption.

Microsoft's Online Services are designed for high availability and to be resilient in the event of in-region failure. Business continuity documentation and planning are subject to annual audits with any material findings documented in the Microsoft Audit Report. In addition, Microsoft provides guidance on how customers can configure their use of Azure to improve their application's resilience.[23]

Against this background, Microsoft recommends that the federal banking agencies recognize in the proposed standards that RTOs are not the only means of addressing service resilience in the context of cloud as well as other online services. Commitments to service availability and downtime can provide covered entities with assurance of service resilience, as those entities consider transitioning workloads to CSPs or other online service providers.

V. Technology Strategies to Mitigate Against Black Swan Scenarios

The ANPR invites comment on improving situational awareness and resilience against cyber attacks, and specifically contemplates a possible requirement that covered entities maintain "secure, immutable, off-line storage of critical records."[24] This invitation suggests that the federal banking agencies may be revisiting traditional ways of thinking about black swan events, including whether traditional off-line storage mechanisms (e.g., off-line tape storage) are the best or only means of maintaining truly secure records.

Black swan events, by their very definition, are not something that can be managed by traditional risk management efforts or technologies alone. Black swan events require the development of management and operational cultures that equip personnel to understand events and make timely decisions to mitigate them. In modern enterprises, this process often involves analytic technologies—such as big data analysis, artificial intelligence, and rapid provisioning of online services. In the end, the best way to mitigate black swan events in the financial sector is through meaningful and regular collaboration between financial institutions, their regulators, and their technology providers. While predicting these events is virtually impossible, the collective expertise of financial institutions, regulators, and technology providers can define the capabilities, capacities, and timelines necessary for effective and timely service recovery and normalization, and can thereby ensure appropriate operational readiness and reliability from both a business and a technical perspective.

Within this context, Microsoft believes that the federal banking agencies will want to be cognizant of the special cyber risk management benefits that large CSPs can offer to the financial services industry in terms of critical operational reliability. Large CSPs encounter and address

[23] See Microsoft Azure, Azure Resiliency Technical Guidance, Aug. 18 2016, available at https://docs.microsoft.com/en-us/azure/resiliency/resiliency-technical-guidance.

[24] See Enhanced Cyber Risk Management Standards, 81 Fed. Reg. 74,324 (Oct. 26, 2016).

cybersecurity risks with much greater regularity and frequency than most, if not all, individual financial institutions and financial market infrastructures. Large CPSs can also bring to bear the most current data analytic technologies to predict cyber events and rapidly respond to imminent or emerging threats. As a result, CSPs often can provide greater system stability and reliability in relation to managing, and greater sophistication in relation to responding to, constantly evolving cyber risks than can most organizations by themselves. This offers an important potential benefit to both financial institutions individually and the financial services industry as a whole—a potential benefit that Microsoft believes the federal banking agencies should not want to unnecessarily impede in their regulatory processes. Ultimately, more secure, more reliable systems of the sort that large CSPs can provide will make black swan events less likely to occur, and more manageable if they should occur.

VI. Conclusion

Microsoft recognizes the importance of the federal banking agencies' efforts, through the proposed standards, to address the critical issues that cyber risk management presents today for regulated financial institutions. Microsoft appreciates the opportunity to provide the foregoing comments in connection with the development of the proposed standards. Microsoft would be happy to address any questions that the federal banking agencies may have regarding its comments or otherwise to assist the agencies in any way it usefully can as the agencies move forward with their development of the standards.

Sincerely,

J. Paul Nicholas

J. Paul Nicholas
Senior Director
Trustworthy Computing
Microsoft Corporation