Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 706 7329
www.microsoft.com

Microsoft

September 21, 2015

VIA EMAIL

Legislative and Regulatory Activities Division
Office of the Comptroller of the Currency
Attention: 1557-0328
prainfo@occ.treas.gov

Re: Microsoft's Comments on the FFIEC Cybersecurity Assessment Tool

Microsoft offers these comments in response to the Federal Financial Institutions Examination Council's (FFIEC) Notice and Request for Comment regarding its Cybersecurity Assessment Tool (the Tool).[1] Microsoft views the Tool as an important and significant step forward in the journey to improve cybersecurity in the financial services sector.

Microsoft commends the FFIEC for producing an assessment methodology that reinforces many cybersecurity risk management practices that Microsoft and other leading technology companies have supported for years, such as use of a secure development lifecycle in application development and replacement of systems that have reached end-of-life (EOL) in favor of modern, more secure systems. Moreover, the Tool promotes regulatory harmonization across the U.S. Government and globally through its mapping to the NIST Cybersecurity Framework, which is a national and international reference point for critical infrastructure cybersecurity. The Tool also provides helpful guidance with respect to threat intelligence and collaboration against cybercrime.

There are a few areas where Microsoft recommends clarifications and improvements to the Tool's current approach that would facilitate a more robust risk assessment and management process for financial institutions. Specifically, Microsoft recommends that the FFIEC revisit its characterization of the inherent risk associated with cloud computing to focus on the cloud service provider's (CSP) compliance and risk management posture, rather than a quantitative assessment of CSPs or binary analysis of different deployment models. Additionally, Microsoft recommends a different approach to cybersecurity attack detection, as the Tool's current language does not reflect the nature of the threat environment.

Microsoft appreciates the opportunity to provide feedback to the FFIEC, and looks forward to continued engagement with the FFIEC and other U.S. Government departments and agencies concerned with cybersecurity.

---

[1] https://www.federalregister.gov/articles/2015/07/22/2015-17907/agency-information-collection-activities-information-collection-renewal-comment-request-ffiec#h-4.

The Tool's Support for Cybersecurity Risk Management Activities

The Tool directly supports several risk management activities that have been critical to improving cybersecurity for Microsoft and other leading technology companies. Microsoft's comments provide further detail about its experiences in the implementation of these activities, with limited recommendations that may help the FFIEC improve its guidance.

Use of a Secure Development Lifecycle

The Tool's Cybersecurity Maturity section properly emphasizes the role of secure development practices. Indeed, the Tool's guidance in the Secure Coding section is consistent with the international standard for secure development, ISO/IEC 27034-1. Microsoft's seven-phase Security Development Lifecycle (SDL) is included as an appendix to this standard,[2] which is demonstrative of Microsoft's commitment to international standardization of cybersecurity practices as well as our leadership on secure development.

The SDL has helped Microsoft and other leading technology companies significantly reduce vulnerabilities in source code. For example, Cisco utilizes a Secure Development Lifecycle, which is modeled after the Microsoft SDL with adaptations to suit Cisco's unique needs.[3] Likewise, Adobe has developed a Secure Product Lifecycle (SPLC), which also draws from the Microsoft SDL with modifications as needed for Adobe.[4]

In future iterations of the Tool, Microsoft recommends that the FFIEC cite ISO 27034 as an informative reference in its discussion of secure coding, in addition to its references to FFIEC Booklets and related guidance. This citation would reinforce the Tool's connections to international standards and industry-tested best practices.

Reliance on End-of-Life Systems

In the Inherent Risk Profile, the Tool appropriately raises concern about reliance on end-of-life (EOL) systems. This is a particularly meaningful area for Microsoft, as new product releases often bring security improvements that cannot reasonably be integrated with prior releases. Simply put, technology users who choose not to upgrade are often making an ill-advised trade-off between short-term cost-avoidance and better cybersecurity risk management.

Consistent with the FFIEC's guidance that organizations should consider upgrading from Windows XP, Microsoft is committed to helping users migrate to newer operating systems.[5,6] XP reached its EOL nearly eighteen months ago, yet reports indicate that approximately 95% of ATMs in the United States still relied on XP nearly six months after Microsoft ended support for XP.[7] Continuing reliance on Windows XP exposes these organizations to significant risk.

---

[2] https://www.microsoft.com/en-us/sdl/
[3] http://blogs.cisco.com/security/the_cisco_secure_development_lifecycle_an_overview
[4] http://blogs.adobe.com/security/2009/05/adobe_reader_and_acrobat_secur.html
[5] http://ithandbook.ffiec.gov/media/154161/final_ffiec_statement_on_windows_xp.pdf
[6] https://www.microsoft.com/en-us/WindowsForBusiness/end-of-xp-support
[7] http://money.cnn.com/2014/03/04/technology/security/atm-windows-xp/

The cloud computing model offers a significant improvement for organizations facing EOL scenarios. An organization that leverages cloud-based software, platforms, and/or infrastructure provided by a trusted CSP would never be using an EOL system because the CSP maintains these systems as current offerings. This enables organizations to refocus their fiscal and human resources on technology priorities and cybersecurity risk management.

Microsoft recommends that the FFIEC continue its emphasis on the risks posed by systems that have reached EOL. Furthermore, Microsoft recommends that the FFIEC point to cloud computing as a technology deployment model that can reduce ongoing challenges associated with EOL systems. For additional input on cloud computing, please see the following section of the document.

Collaboration Against Cybercrime

The Tool's Cybersecurity Maturity section provides helpful guidance to institutions regarding the importance of threat intelligence and collaboration against cybercrime. Microsoft's Digital Crimes Unit is an active supporter of the financial services community in these efforts, including through partnership with FS-ISAC.[8] For example, Microsoft worked with financial services institutions and law enforcement organizations to disrupt the Citadel and Caphaw botnets. These anti-botnet actions demonstrate both the global nature of cybercrime and the need for cross-sector partnership to mitigate cyber-threats.

Microsoft commends the FFIEC's guidance to join or subscribe to threat and vulnerability sharing source(s), such as FS-ISAC. Microsoft also commends the FFIEC's guidance to formally establish – and continually invest in – a threat intelligence program. Taken together with the breadth of risk management guidance provided in the Tool, these steps can significantly aid an organization's journey to improved cybersecurity and resilience in today's complex threat environment.

Areas for Further Development of the Tool

There are sections of the Tool where further development would improve the quality of its cybersecurity risk management guidance. Microsoft's comments identify these areas and provide specific recommendations about potential improvements.

Characterization of Cloud Computing's Inherent Risk

Microsoft recommends that the FFIEC reconsider its characterization of the inherent risk associated with cloud computing. The Tool's current approach focuses on quantitative factors, such as the number of CSPs utilized by an organization, and binary deployment considerations, namely whether an organization uses public or private cloud, or leverages domestic or overseas data centers. The Tool also states that an absence of cloud services presents no inherent risk when weighed against the option of using cloud services, but this is only true in instances where the on-premise system has been designed, built, operated, and maintained to meet the strict requirements for integrity, security, availability, privacy and confidentiality objectives which many cloud services are designed to meet. As an alternative to these assessments, the Tool should focus its guidance on the CSP's capability to demonstrate that it can deliver a trusted cloud.

[8] http://blogs.microsoft.com/on-the-issues/2014/09/29/microsoft-partners-financial-services-industry-fight-cybercrime/

There are at least two threshold risk management questions that should inform revision of the Tool. The key question facing financial services institutions in their migration to cloud services is whether the CSP meets minimum international and national standards that address cybersecurity and privacy, such as the 27001 series (e.g., ISO/IEC 27001 and 27018), the SOC standards (e.g., SSAE16 SOC II), and FFIEC guidance. This should be the minimum bar for financial services institutions considering cloud services. Moreover, highlighting these compliance and certification activities would be consistent with the Tool's approach to Cybersecurity Maturity, in which certain audit practices outlined in the FFIEC's Audit, Information Security, and Operations Booklets (e.g., third-party assessment, etc.) provide the baseline level of maturity.

Another important risk management question is whether the CSP has a programmatic approach to transparency into its service architecture, operations, and features through ongoing customer engagement, outside of the sales cycle. Such transparency is critical to enabling thorough risk assessment by the financial services institution, both during the initial phases of a cloud deployment and as the organization matures in its use of cloud services.

With regard to the statement that no cloud usage poses the least risk to an organization, cloud security teams are often better resourced and have significantly greater clarity of focus in their mission than in-house IT teams, which often do not have comparable resources and face many competing demands. This is particularly true when the cloud user is a smaller institution and the CSP is a deeply experienced and well-resourced provider.

Additionally, the Tool includes "use of public cloud" as a descriptive element of inherent risk only in the two highest levels of risk (Significant and Most), while "private cloud only" is associated with a lower level (Minimal). In fact, while private cloud deployments may offer greater customization for the cloud user, it is a more costly model that may be out of reach for smaller institutions. As a result, these institutions may choose to rely upon in-house IT teams that may have less security capability than the CSP's teams that support public, multi-tenant cloud services. Alternatively, the Tool should encourage institutions to explore whether the CSP can support deployment models that enable continued on-premise management of certain organizational assets.

For these reasons, Microsoft offers proposed language for consideration in further revision of the Tool. In Microsoft's view, this proposed language provides financial services institutions with actionable and risk-based guidance to help assess and properly manage their inherent risk as they consider migration to cloud services.

Category: Technologies and Connection Types	Risk Levels				
	Least	**Minimal**	**Moderate**	**Significant**	**Most**
Cloud computing services hosting externally to support critical activities	Cloud service provider(s) (CSP) have been audited by a third-party against international and national security and risk management standards; CSP(s) provide programmatic transparency into service architecture, operations, and features; CSP(s) provide "hybrid" cloud deployment models that enable ongoing use of on-premise IT systems; CSP(s) operate enterprise risk management program.	CSP(s) have been audited by a third-party against international and national security and risk management standards; CSP provides programmatic transparency into service architecture, operations, and features; CSP(s) provide "hybrid" cloud deployment models that enable ongoing use of on-premise IT systems.	CSP(s) offer self-attestation(s) against international and/or national security and/or risk management standards.	CSP(s) have only mapped their security controls to international and/or national security and/or risk management standards.	CSP(s) cannot articulate adherence to international and/or national security and/or risk management standards; CSP(s) does not have programmatic approach to transparency into service architecture, operations, and features; CSP(s) does not have enterprise risk management program.

Characterization of Attempted Cyber Attacks

Microsoft recommends that the FFIEC reconsider its characterization of the inherent risk associated with attempted cyber attacks. The Tool's current approach communicates that an organization that does not detect attempted cyber attacks has the least inherent risk. The problem with this approach is that there is not a financial services institution in the world today that does not experience attempted cyber attacks of some type. An organization that does not identify cyber attacks is simply not detecting them, which carries more risk than detection of constant attempted attacks.

The better approach would be to assume some level of attempted attacks in the Inherent Risk Profile, and then bring both quantitative and qualitative factors into the risk assessment and mitigation process. The Cybersecurity Maturity section of the Tool – namely the Cybersecurity Controls and the Cyber Incident Management and Resilience Domains – provide a broad range of helpful steps that organizations should leverage to protect, detect, and respond to attempted cyber attacks.

Another important consideration in recasting the inherent risk associated with attempted cyber attacks is the nature of the attacker. The role of nation-state actors and their politically-motivated proxies should be clearer, as financial services institutions have emerged as among the primary target of governments seeking to destabilize their geopolitical opponents. For example, Members of Congress have publicly implicated the Iranian government in Distributed Denial of Service (DDos) attacks against U.S. banks,[9] and the Syrian Electronic Army's posting of false information on a widely-followed Twitter account resulted in an immediate loss of $136 billion in the U.S. stock market.[10] These attacks against critical infrastructure run counter to normative behavior for nation-states in cyberspace – or cybersecurity norms – that have been endorsed by the U.S. government, the Shanghai Cooperation Organization, the United Nations Group of Governmental Experts, the Organization for Security and Cooperation in Europe, and Microsoft.

For these reasons, Microsoft offers proposed language for revision of the Tool. This proposed language retains much of the FFIEC's original language by shifting all depictions to the left (i.e., the FFIEC's original language for Minimal Risk is proposed for Least Risk, and so on). This proposed language also presents a new depiction of Most Risk that specifically notes the role of nation-state and/or politically-motivated proxies.

[9] https://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html

[10] https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/

	Risk Levels				
	Least	**Minimal**	**Moderate**	**Significant**	**Most**
Detection of attempted cyber attacks	Few attempts monthly (<100); may have had generic phishing campaigns received by employees and customers	Several attempts monthly (100–500); phishing campaigns targeting employees or customers at the institution or third parties supporting critical activities; may have experienced an attempted Distributed Denial of Service (DDoS) attack within the last year	Significant number of attempts monthly (501–100,000); spear phishing campaigns targeting high net-worth customers and employees at the institution or third parties supporting critical activities; Institution specifically is named in threat reports; may have experienced multiple attempted DDoS attacks within the last year	Substantial number of attempts monthly (>100,000); persistent attempts to attack senior management and/or network administrators; frequently targeted for DDoS attacks	All characteristics of Significant Risk, plus warning from government authorities or other comparably informed sources that the institution is being targeted by nation-state actors and/or their politically-motivated proxies

Conclusion

Microsoft appreciates the opportunity to provide these comments and would welcome an opportunity to elaborate on its perspective with FFIEC representatives.

Sincerely,

J. Paul Nicholas
Senior Director
Microsoft Global Security Strategy and Diplomacy
Trustworthy Computing