**Content Partner Risk Management Program (CPRM)**

**Scan Compliancy FAQ**

**February 1st, 2010**

The questions and answers below are designed to answer the most common questions regarding the Scan Compliancy form. If you have additional questions, please contact [CPRM@microsoft.com](mailto:CPRM@microsoft.com)

**Q: Which partners are impacted by this requirement?**

A: All CPRM partners (new and existing) are required to sign the Scan Compliancy form to acknowledge that scans will be occurring.

**Q: Why is this requirement being implemented?**

A: Initially, the SLA/Security Exhibit was used to communicate the scan requirement for partners. However, in recent months there has been a clear indication that the CPRM program needed to implement a formalized acknowledgement for the scanning that is performed for partners.

**Q: Who is excluded from this new requirement?**

A: The following deal types are excluded from completing the Scan Compliancy form:

* Akami hosted deals

**Q: Does my partner have to sign a Scan Compliancy form for each type of scan being performed?**

A: No. The Scan Compliancy form is a blanket acknowledgement that scans will be performed on the site. This includes initial onboarding and ongoing host scans and web application scans.

**Q: How much time will a Scan Compliancy Form add to the on-boarding process in CPRM?**

A: If a signed Scan Compliancy Form is sent to the CPRM Business Desk at the time the SLA is submitted, no additional time should be expected to process the request (not withstanding vulnerability resolutions and rescans). However, if the scan request is submitted *without* the signed Scan Compliancy Form or SLA, then the request will not be processed until BOTH forms are received.

**Q: What if my partner refuses to sign the Scan Compliancy Form or needs more information about the scan itself?**

A: Explain to the partner that scanning a site is a requirement mandated by Online Services Security & Compliancy (OSSC). Additional information about the scanning requirements can be found in the Security Exhibit (contained within the SLA) which can be obtained from the [CPRM Business Desk.](mailto:cprm)

If the Partner still insists on more granular information about the scanning process, please escalate to the CPRM Business Desk. We will, in turn, put the Partner and the MS Business owner in contact with the OSSC Scanning team.

**Q: What if a partner reuses a previously scanned URL?**

A:  If the IP or URL was scanned less than 30 days earlier via a different request (wherein a Scan Compliancy Form was also submitted to and approved by CPRM) then an additional Scan Compliancy Form is not required.

**Q: Will notifications be sent out at the start of each scan?**

A: Yes and No. Host scans are performed on a regular basis without notification. However, if a partner site qualifies for web application scanning (this includes both full and light versions) a notification will be sent prior to the web application scan being performed.

**Q: Who should be aware of the scans being performed?**

A: Any partner hosting a Microsoft co-branded site must be aware and acknowledge the scans being performed. The formal acknowledgement is recorded via the Scan Compliancy form. In addition, partners must advise the appropriate IT staff for the partner site that scans will be performed to ensure that the scans we perform are not mistaken for an attack on the site.

**Q: What if my existing partner doesn’t want to sign the Scan Compliancy Form?**

A: The SLA/Security Exhibit states that a scan is required. This form simply records the acknowledgement of the scan requirement. If a Partner refuses to sign the Scan Compliancy Form, LCA escalations will occur.