Dear Wendy,

On behalf of the Web Application Security WG, we would like to request a meeting with the Director to approve advancement of Content Security Policy (CSP) Level 2 to Candidate Recommendation status.

The specification is expected to Proposed Recommendation no earlier than July 1st, 2015 as only one complete implementation exists at this time.

At the time of transition to Candidate Recommendation of CSP Level 2, the WG has also resolved, during our F2F at TPAC 2014, to obsolete CSP Level 1 by transitioning it to a Working Group Note.

1. Record of the group's decision to request advancement

A Call for Consensus was issued to public-webappsec@w3.org on October 20th (http://lists.w3.org/Archives/Public/public-webappsec/2014Oct/0063.html) and completed successfully. After Last Call had completed, the group received additional substantive feedback which we agreed to delay advancement in order to address.

After this extended resolution period, a second Call for Consensus was issued on Jan 27 (https://lists.w3.org/Archives/Public/public-webappsec/2015Jan/0266.html) and a decision to advance to CR was ratified on the group's regular teleconference on February 9 and recorded in the minutes available at:

http://www.w3.org/2011/webappsec/draft-minutes/2015-02-09-webappsec-minutes.html

2. Public documentation of all substantive changes to the technical report since the previous publication.

A summary of changes from version 1.0 is available in the document itself as part of the Introduction.

Since the document was published as a Last Call Working Draft, the following substantive changes have been made. These GitHub changelogs are available to the general public.

https://github.com/w3c/webappsec/commit/c39f73a5fd93dd68de228a2e8914734c8e14a16c#diff-efb7158bc46add0164a355e6ad881a1f
Drop literal IPv4 support apart from 127.0.0.1

https://github.com/w3c/webappsec/commit/6f89d89bd4965040b9ad30bb8b7ed0105fe4ae10#diff-efb7158bc46add0164a355e6ad881a1f
Defer 'reflected-xss' directive to Level 3

https://github.com/w3c/webappsec/commit/d8fee06f18d96ccd7cb6e8cbdf144878560459d5#diff-efb7158bc46add0164a355e6ad881a1f
Move ‘referrer’ directive to referrer policy spec

https://github.com/w3c/webappsec/commit/aba91ac272ce02a8948aeeab6bca1d9aa109d990#diff-efb7158bc46add0164a355e6ad881a1f
Note that IP addresses match ‘self’

https://github.com/w3c/webappsec/commit/50cd0920cfba1a7d7b84659862eb24a44b4ca459#diff-efb7158bc46add0164a355e6ad881a1f
Clarify that owner document can also apply to parent worker for enforcement.

https://github.com/w3c/webappsec/commit/0d204ac3ede6fb48659efb11282909494fda756d#diff-efb7158bc46add0164a355e6ad881a1f
Clarify sandbox behavior as it applies to workers

https://github.com/w3c/webappsec/commit/b52c77b82b14ec7b619708543f5f9507215548a7#diff-efb7158bc46add0164a355e6ad881a1f
Drop support for IPv6 addresses

https://github.com/w3c/webappsec/commit/d2925a289c9c6aa39c5600b325aed4923c89455a#diff-efb7158bc46add0164a355e6ad881a1f
Path parsing algorithm updates

https://github.com/w3c/webappsec/commit/788107732af4db10ecfb3be50de9ae7a2a6b60a5#diff-efb7158bc46add0164a355e6ad881a1f
case-insensitive comparisons are done in ASCII

https://github.com/w3c/webappsec/commit/8cbfd691843b110f97b522e06c2990b532d477dd#diff-efb7158bc46add0164a355e6ad881a1f
Explicitly list schemes that do not match ‘*’

https://github.com/w3c/webappsec/commit/35aa6f7674c22c3178f6d67d98c0602ff509f65e#diff-efb7158bc46add0164a355e6ad881a1f
Explicitly allow multiple <meta> policies

https://github.com/w3c/webappsec/commit/6c0c6a26c21dd9e664a6770ad05033a0ace4e064#diff-efb7158bc46add0164a355e6ad881a1f
Clarify behavior around Link header and prefetching

https://github.com/w3c/webappsec/commit/7b3b425ae340734a088323ff2ffb7f575d7e3163#diff-efb7158bc46add0164a355e6ad881a1f

Match hash productions with SRI productions

https://github.com/w3c/webappsec/commit/fd7e1a2f602d3528efb5c292fda9b7912448b2bb#diff-efb7158bc46add0164a355e6ad881a1f
Note that ‘base-uri’ does not fallback to ‘default-src’

https://github.com/w3c/webappsec/commit/ae22342195ef00120c2a0d1ec1edb47b03bc5681#diff-efb7158bc46add0164a355e6ad881a1f
Clean up URL parsing

https://github.com/w3c/webappsec/commit/f2f6ec23dfc8cedbc523b4ead5a2eab39ce82c79#diff-efb7158bc46add0164a355e6ad881a1f
Clarify ‘frame-ancestors’ behavior with regard to friendly error pages

https://github.com/w3c/webappsec/commit/3e856006a34d9f75d28d696c510f055084567c29#diff-efb7158bc46add0164a355e6ad881a1f
Clarifications of <meta> enforcement and placement

https://github.com/w3c/webappsec/commit/3e856006a34d9f75d28d696c510f055084567c29#diff-efb7158bc46add0164a355e6ad881a1f
Nonces SHOULD be 128 bits and cryptographically random

https://github.com/w3c/webappsec/commit/971dd0916a7dcb558d3433278203c6930902c281#diff-efb7158bc46add0164a355e6ad881a1f
‘sandbox’ directive does not have reporting requirements on violations

https://github.com/w3c/webappsec/commit/682b69cf4d73e47b155a2ddd778d4ed7fe0f04ae
Hostnames with a trailing ‘.’ do not match hostnames without.

https://github.com/w3c/webappsec/commit/bdc66b7b704a944f4b0a03cfc79fb91c6fa31d65
‘frame-ancestors’ directive ABNF updated to disallow path components

https://github.com/w3c/webappsec/commit/7cbaa4e67079c47eeaafa94ac6f71764db3406f0
‘child-src’ and ‘CSP’ client hint headers marked as AT RISK

https://github.com/w3c/webappsec/commit/c2fdd7f338db13b90f37000e1287bca115404724
nomenclature fix for ‘token’ vs ‘policy’ in describing referrer directive

https://github.com/w3c/webappsec/commit/148e8adb3b8b4c874aa5681cb63b723d4eef87f2
add “parse a group of selectors” for processing CSSOM blocking

https://github.com/w3c/webappsec/commit/b48b635f93a798da87c61e5b8c2d89d8b36567d8
https://github.com/w3c/webappsec/commit/d5483ae3cb199798cdd44d5c85c2482e7f992501

make definition of referrer policies explicit and delegate to the REFERRER spec

https://github.com/w3c/webappsec/commit/570ca5210a5055110acf3894978ace0333e048a2
typos in sandbox directive ABNF fixed

https://github.com/w3c/webappsec/commit/6381b4e1117da9cdbd966e255909601835640473
note that Beacon is covered by connect-src directive, not form-action

3. Features AT RISK

CSP request header, which indicates to a server that a CSP policy is being enforced so it might, e.g. decline to issue a redirect which could leak information about e.g. the logged-in state of the user

4. Evidence that all issues raised about the document since Last Call Working Draft have been formally addressed:

CfC to advance to LCWD was issued on June 11th: http://lists.w3.org/Archives/Public/public-webappsec/2014Jun/0125.html. Issues raised directly in that thread were resolved before publishing the draft. A few questions and issues were raised on the list post-publication, and resolved as follows:

1. http://lists.w3.org/Archives/Public/public-webappsec/2014Jun/0162.html suggested that 'referrer' and 'reflected-xss' ought to be part of some other header. That thread died at http://lists.w3.org/Archives/Public/public-webappsec/2014Jun/0178.html. We should probably "formally address" it in some way.
2. http://www.w3.org/2011/webappsec/track/issues/61 was raised (also as http://www.w3.org/2011/webappsec/track/issues/62). I think the answer is no, but it hasn't been formally closed.
3. Dan raised http://lists.w3.org/Archives/Public/public-webappsec/2014Jun/0187.html and more or less withdrew it at http://lists.w3.org/Archives/Public/public-webappsec/2014Jun/0201.html
4. We changed the name to Level 2: http://lists.w3.org/Archives/Public/public-webappsec/2014Jun/0203.html
5. Neil proposed a 'report-only' field in http://lists.w3.org/Archives/Public/public-webappsec/2014Jun/0218.html. Discussed at TPAC and responded with: http://lists.w3.org/Archives/Public/public-webappsec/2014Nov/0041.html
6. http://lists.w3.org/Archives/Public/public-webappsec/2014Jun/0236.html was resolved in http://lists.w3.org/Archives/Public/public-webappsec/2014Jun/0241.html with no change to the spec.

7. http://lists.w3.org/Archives/Public/public-webappsec/2014Jun/0252.html is punted to CSP3.
8. http://lists.w3.org/Archives/Public/public-webappsec/2014Jul/0018.html trailed off in http://lists.w3.org/Archives/Public/public-webappsec/2014Jul/0020.html and http://www.w3.org/2011/webappsec/draft-minutes/2014-07-16-webappsec-minutes.html#item03. This is tracked by fetch integration plans for CSP 3.
9. http://lists.w3.org/Archives/Public/public-webappsec/2014Jul/0061.html re-raised the question of extensions: resolved in http://lists.w3.org/Archives/Public/public-webappsec/2014Jul/0069.html and
10. http://lists.w3.org/Archives/Public/public-webappsec/2014Jul/0073.html suggested new syntax. Punted to CSP3.
11. http://lists.w3.org/Archives/Public/public-webappsec/2014Jul/0083.html suggested dealing with ServiceWorkers. Punted to the SW spec. Might bring it into CSP3.
12. http://lists.w3.org/Archives/Public/public-webappsec/2014Jul/0113.html 'unsafe-inline' for SVG images? Trailed off at http://lists.w3.org/Archives/Public/public-webappsec/2014Jul/0123.html Addressed with no change at http://www.w3.org/2014/10/27-webappsec-minutes.html#item10
13. I broke the sandbox ABNF and fixed it (twice) in http://lists.w3.org/Archives/Public/public-webappsec/2014Aug/0018.html
14. http://lists.w3.org/Archives/Public/public-webappsec/2014Aug/0021.html punted to CSP3 as http://www.w3.org/2011/webappsec/track/issues/64
15. mnot's suggestions at http://lists.w3.org/Archives/Public/public-webappsec/2014Aug/0028.html resulted in a few spec changes.
16. http://lists.w3.org/Archives/Public/public-webappsec/2014Aug/0031.html resulted in http://lists.w3.org/Archives/Public/public-webappsec/2014Aug/0038.html
17. http://lists.w3.org/Archives/Public/public-webappsec/2014Aug/0032.html resulted in http://lists.w3.org/Archives/Public/public-webappsec/2014Aug/0037.html
18. http://lists.w3.org/Archives/Public/public-webappsec/2014Aug/0015.html punted to CSP 3 by http://lists.w3.org/Archives/Public/public-webappsec/2014Nov/0038.html
19. http://lists.w3.org/Archives/Public/public-webappsec/2014Aug/0034.html punted to CSP3 as https://github.com/w3c/webappsec/issues/44
20. http://lists.w3.org/Archives/Public/public-webappsec/2014Aug/0049.html resolved in http://lists.w3.org/Archives/Public/public-webappsec/2014Aug/0051.html with no spec changes
21. http://lists.w3.org/Archives/Public/public-webappsec/2014Aug/0050.html resolved in http://lists.w3.org/Archives/Public/public-webappsec/2014Aug/0109.html with no spec changes.
22. http://lists.w3.org/Archives/Public/public-webappsec/2014Aug/0146.html is addressed by http://lists.w3.org/Archives/Public/public-webappsec/2014Nov/0040.html.
23. http://lists.w3.org/Archives/Public/public-webappsec/2014Aug/0143.html resulted un making child-src at risk (though I still don't understand the objection). TPAC call for consensus completed with no objections from Dan on this.

24. http://lists.w3.org/Archives/Public/public-webappsec/2014Aug/0151.html was fixed in the spec.
25. http://lists.w3.org/Archives/Public/public-webappsec/2014Aug/0154.html resulted in the addition of a "changes from 1.0" section to the spec.
26. http://lists.w3.org/Archives/Public/public-webappsec/2014Aug/0159.html resulted in a small bug fix to the CSSOM bits of the spec.
27. http://lists.w3.org/Archives/Public/public-webappsec/2014Aug/0162.html is punted to CSP3 as https://www.w3.org/2011/webappsec/track/issues/67
28. ISSUE-65 was a typo, resolved in the spec.

5. Formal Objections

None.

6. Public documentation of changes that are not substantive.

All commits are publicly visible at:
https://github.com/w3c/webappsec/commits/master/specs/content-security-policy

7. Which, if any, of the Working Group's requirements for this document have changed since the previous step:

None.

8. Any changes in dependencies with other groups.

No significant changes. CSP Level 2 references the following specifications which are not at Candidate Recommendation or equivalent. We believe that conformant implementations are unlikely to be impacted by foreseeable changes to these specifications, as follows:

Beacon
http://www.w3.org/TR/beacon/
No impact If the spec is abandoned or “sendBeacon()” method is removed. If the name is changed but the feature remains the same, implementers will need to update if they wish the feature to still be covered by CSP connect-src. Internal implementation changes to the method will not impact CSP.

CSS3 Fonts
http://www.w3.org/TR/2013/WD-css3-fonts-20130212/
No impact If the spec is abandoned or <@font-face> CSS rule is removed. If the name is changed but the feature remains the same, implementers will need to update if they wish the

feature to still be covered by CSP style-src. Internal implementation changes to the method will not impact CSP.

CSS4 Images
http://www.w3.org/TR/2012/WD-css4-images-20120911/
No impact If the spec is abandoned or <image()> or <image-set()> CSS rules are removed. If the name is changed but the feature remains the same, implementers will need to update if they wish the feature to still be covered by CSP style-src. Internal implementation changes to the method will not impact CSP.

CSSOM
http://www.w3.org/TR/2011/WD-cssom-20110712/
At risk: 'unsafe-eval' token for style-src is used to guard mutations via the CSSOM. If this spec is abandoned or the feature is removed, these rules in CSP will be no-op, but any risk will also be removed.

HTML Imports
http://www.w3.org/TR/html-imports/
Imports are governed by "script-src" which is the most critical directive for meaningful security. Changes to the internals of the specification will not impact CSP or the security posture provided.

URL
http://www.w3.org/TR/url/
The spec defines URL by reference to this specification, and uses the result of processing a URL through the URL Parser defined by it to determine if source expressions match. References to the scheme, host, port and path portions of the result of parsing a URL are used. These are all extremely stable concepts, fundamental to the Web, which cannot change without fundamental breakage of how browsers work. Internal implementation details of the URL Parser algorithm will not require conformance changes in CSP implementations, and it is critical that the handling of this comparison use the browser's internal view of parsed URLs for Fetch and other operations rather than any more stable algorithm which might yield results inconsistent from Fetch behavior.

XMLHttpRequest
http://www.w3.org/TR/2012/WD-XMLHttpRequest-20121206/
Is de-facto stable though not formally advanced beyond WD.

9. Implementations known to the Working Group

A relatively complete implementation of Level 2 is available in Chromium since version 40.

Firefox supports all of the Level 1 behavior.

Chrome and Firefox both have public support for hash-source and nonce-source enabled.

Internet Explorer is implementing at least all Level 1 directives with Level 2 behaviors where any conflicts exist and this is available in the developer channel now. Support for all Level 2 directives has not been announced but there has been no objection or declared intent not to implement any particular directives.

10. Documentation of Implementation Experience

The WG is developing a test suite as part of the Web Platform Tests effort and it can be run at:

http://w3c-test.org/tools/runner/index.html?path=/content-security-policy