BCR

BERLINER CORCORAN & ROWE LLP

Regulatory Alert **April 6, 2021**

BIS Significantly Reduces Burden of Encryption Reporting Requirements and Liberalizes Certain Other Encryption Controls

Effective March 29, 2021, the Bureau of Industry and Security ("BIS") made significant changes to its export/reexport controls on encryption items. These changes were part of a BIS final rule that amended the Export Administration Regulations ("EAR") to implement changes made by the Wassenaar Arrangement in December 2019. 86 Fed. Reg. 16482 (March 29, 2021). The Wassenaar Arrangement is an international export control regime that has 42 member states, including the United States. The Alert discusses the most significant changes.

1. No Notification Required for Most Publicly Available Encryption Source Code. Previously, open source encryption items required an e-mail notification to BIS and NSA in order to release it from EAR jurisdiction. This rule narrows the EAR § 742.15(b)(2) notification requirement to apply only to such source code that provides or performs "non-standard cryptography." BIS estimates that this change will result in an 80% reduction in these notifications.

As before, EAR § 772.1 defines "non-standard cryptography" to mean "any implementation of `cryptography' involving the incorporation or use of proprietary or unpublished cryptographic functionality, including encryption algorithms or protocols that have not been adopted or approved by a duly recognized international standards body (e.g., IEEE, IETF, ISO, ITU, ETSI, 3GPP, TIA, and GSMA) and have not otherwise been published."

2. Beta Test Encryption Software. Likewise, BIS revised the License Exception TMP provision in EAR § 740.9(c)(8) to require notification only for beta test software that provides or performs "non-standard cryptography."

3. Mass Market Encryption Hardware and Software. The rule modified EAR § 740.17(e)(3) to eliminate the self-classification reporting requirement for all mass market encryption hardware and software that qualified for EAR § 740.17(b)(1) before March 29, 2021. Specifically, companies are no longer required to report to BIS and the ENC Encryption Request Coordinator their self-classifications under 5A992.c and 5D992.c of hardware and software, respectively, that meet the criteria of Note 3 to Category 5 – Part 2 of the Commerce Control List ("CCL"). This covers a broad range of encryption end-items, such as application software, PCs and other consumer products.

As before, mass market encryption hardware and software are ineligible for self-classification under EAR § 740.17(b)(1) if they (i) are described in EAR § 740.17(b)(2), (ii) provide or perform "non-standard cryptography", or (iii) are "cryptographic activation" hardware or software.

Export Controls and Sanctions Group

Benjamin Flowe, Jr.

John Ordway

Daniel Fisher-Owens

Babak Hoghooghi

Perry Bechky

David Baron

Ray Gold

Michelle Roberts

Jason McClurg

Contact Ray Gold (raygold@bcr-dc.com), Dan Fisher-Owens (dfo@bcr-dc.com), Ben Flowe (bflowe@bcr-dc.com), or your regular BCR contact for more details.

1101 17th Street NW, Suite 1100, Washington, DC 20036
+1-202-293-5555 www.bcr.us

4. Mass Market Chips, Chipsets, Electronic Assemblies and Field Programmable Logic Devices, and Their Qualifying 'Executable Software.' The rule moved mass market chips, chipsets, electronic assemblies, field programmable logic devices, and their qualifying 'executable software' from EAR § 740.17(b)(3)(i) to EAR § 740.17(b)(1). As a result, such items can now be self-classified under 5A992.c (hardware) or 5D992.c (software) if they meet the criteria of Note 3 to CCL Category 5 – Part 2. However, self-classification reporting is still required for such items. Formal BIS classifications of such items are no longer required if they: (i) are not described in EAR § 740.17(b)(2), (ii) do not provide or perform "non-standard cryptography", and (iii) are not "cryptographic activation" hardware or software.

5. Mass Market Development Kits (Toolsets) and Toolkits. Likewise, mass market development kits (toolsets) and toolkits that are standalone products (e.g., are not components or 'executable software' of another mass market product) are now also authorized under EAR § 740.17(b)(1). Thus, these kits and toolkits can be self-classified under ECCN 5A992.c or 5D992.c if they meet the criteria of Note 3 to CCL Category 5 – Part 2. Self-classification reporting is not required. Formal BIS classifications of such kits and toolkits are no longer required if they: (i) are not described in EAR § 740.17(b)(2), (ii) do not provide or perform "non-standard cryptography", and (iii) are not "cryptographic activation" hardware or software.

While cryptographic libraries and modules in EAR § 740.17(b)(3)(i)(B) can also qualify for EAR § 740.17(b)(1), BIS expects that most cryptographic libraries and modules will remain in EAR § 740.17(b)(3)(i)(B) because Note 3 to CCL Category 5 – Part 2 excludes items whose primary function or set of functions is "information security."

BIS estimates that these revisions (3 – 5 above in this Alert) will result in a 60% reduction in encryption self-classification reports.

The March 29, 2021, rule made no changes to the classification or self-classification reporting requirements for encryption items controlled under 5A002, 5B002, and 5D002. These ECCNs control non-mass market encryption items subject to the EAR that do not qualify for an exclusion to CCL Category 5 – Part 2.

6. Wireless Personal Area Networks. BIS expanded the scope of 5A002.a exclusion Note 2, paragraph f, by removing the limitations on operating range and number of connections. Consequently, paragraph f now excludes from CCL Category 5 – Part 2 any "[i]tems where the `information security' functionality is limited to wireless `personal area network' functionality implementing only published or commercial cryptographic standards." Also, BIS amended the definition of "personal area network" in EAR § 772.1 to clarify that a "local area network" is not a "personal area network."

7. Exclusion for Operations, Administration or Maintenance. BIS expanded the scope of 5A002.a exclusion Note 2, paragraph h to add gateways, so that paragraph h now reads: "Routers, switches, gateways or relays, where the `information security' functionality is limited to the tasks of `Operations, Administration or Maintenance' (`OAM') implementing only published or commercial cryptographic standards."