AN A.S. PRATT PUBLICATION
FEBRUARY-MARCH 2022
VOL. 8 NO. 2

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 8 **NUMBER 2** **February-March 2022**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [8] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [2] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2022–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Intrusion Preclusion: BIS Issues Long-Awaited Controls on Cybersecurity Items, Creates New License Exception

By Josephine I. Aiello LeBeau and Anne E. Seymour*

The Department of Commerce's Bureau of Industry and Security has issued an interim final rule implementing expanded export controls on cybersecurity items. The authors of this article discuss the interim final rule.

The Department of Commerce's Bureau of Industry and Security ("BIS") has issued an interim final rule (the "Rule") implementing expanded export controls on cybersecurity items based on the belief that these items "could be used for surveillance, espionage, or other actions that disrupt, deny or degrade the network or devices on it." The new controls on cybersecurity items stem from the 2013 addition by the Wassenaar Arrangement[1] ("WA") of cybersecurity items, including intrusion software to Wassenaar's list of controlled items. Public comments in 2015 indicating significant concerns over BIS's implementation and scope of the proposed controls resulted in renegotiation of these controls at the WA's 2017 meeting.

The Rule implements the WA 2017 controls. The Rule is intended to prevent malicious "intrusion software" from being exported to certain countries of concern without a BIS license and not to hinder responses to cybersecurity flaws and incidents.

NEW CYBERSECURITY RELATED ECCNS

The Rule creates new controls on hardware and software Export Control Classification Numbers ("ECCN") (4A005 and 4D004, respectively) specially designed or modified for the generation, command and control, or delivery of intrusion software. The Export Administration Regulations ("EAR") define intrusion software as software specially designed or modified to avoid detection by monitoring tools[2] or to defeat protective

* Josephine I. Aiello LeBeau is a partner at Wilson Sonsini Goodrich & Rosati, advising clients on compliance and enforcement of U.S. export control regulations and economic sanctions, and analyzing international transactions and enforcement matters, novel business prospects, and ongoing compliance-related issues. Anne E. Seymour is counsel at the firm, where she focuses on issues related to compliance and enforcement of U.S. export control regulations and economic sanctions and U.S. import regulations. Resident in the firm's office in Washington, D.C., the authors may be reached at jalebeau@wsgr.com and aseymour@wsgr.com, respectively.

[1] The Wassenaar Arrangement is voluntary export control regime whose 42 member states exchange information on transfers of and maintain a multilateral control list of conventional weapons and dual-use goods and technologies.

[2] Monitoring tools are defined as software or hardware that monitors system behaviors or processes running on a device. This includes antivirus ("AV") products, end point security products, Personal Security Products ("PSP"), Intrusion Detection Systems ("IDS"), Intrusion Prevention Systems ("IPS"), or firewalls.

countermeasures,[3] of a computer or network capable device (such as a mobile device or smart meter). Intrusion software either (1) extracts data or information (from the computer or network-capable device) or modifies system or user data, or (2) modifies the standard execution path of a program or process in order to allow the execution of externally provided instructions.

According to the proposed Rule, it does not include any of the following: Hypervisors, debuggers or Software Reverse Engineering ("SRE") tools; Digital Rights Management ("DRM") software; or software designed to be installed by manufacturers, administrators, or users, for the purposes of asset tracking or recovery.

The Rule also adds paragraph 5A001.j "IP network communications surveillance systems or equipment" to ECCN 5A001 which is similar to controls on software that currently exist in ECCN 5D001.e.

Finally, the Rule adds new controls (subcategories to ECCN 4E001) on technology related to these newly added items and technology for the development of intrusion software. The controls generally exclude information needed to respond to, rather than cause, a cybersecurity incident[4] or disclose a vulnerability.[5]

NEW LICENSE EXCEPTION

The newly added ECCNs are controlled for national security ("NS") reasons, which means that a license or license exception would be required to export the items to most destinations. The new Rule establishes a new License Exception, Authorized Cybersecurity Exports ("License Exception ACE" or "ACE"), which according to BIS will "avoid impeding legitimate cybersecurity research and incident response activities." License Exception ACE will allow the export of cybersecurity items to many destinations.[6] In addition to the country-based controls, License Exception ACE cannot be used when the exporter has reason to know that the item "will be used to affect the confidentiality, integrity or availability of information or information systems."

---

[3] Protective countermeasures are defined as techniques designed to ensure the safe execution of code, such as Data Execution Prevention ("DEP"), Address Space Layout Randomization ("ASLR"), or sandboxing.

[4] Cyber incident response means the process of exchanging necessary information on a cybersecurity incident with individuals or organizations responsible for conducting or coordinating remediation to address the cybersecurity incident.

[5] Vulnerability disclosures include the process of identifying, reporting, or communicating a vulnerability to, or analyzing a vulnerability with, individuals or organizations responsible for conducting or coordinating remediation for the purpose of resolving the vulnerability.

[6] For a detailed description of ACE eligibility, please see the table herein.

NEXT STEPS

Again, the Rule is intended to prevent disruptive "intrusion software" from being exported to certain countries of concern without a BIS license, rather than to hinder responses to cybersecurity flaws and incidents. However, to the extent that the new controls are overly broad, the Rule specifies that there is a 45-day comment period (which ended December 6, 2021). The Rule will become effective 90 days from its publication in the Federal Register (January 19, 2022).

Country Group	ACE Restrictions	Exception to restrictions
B	None – May use ACE to these countries.	
D:1	No government end-users; no non-government end-users	EXCEPTION: (1) Exports, reexports or transfers (in-country) of ECCNs 4A005, 4D001.a (for 4A005 or 4D004), 4D004, 4E001.a (for 4A005), 4D001.a (for 4A005 or 4D004) to "favorable treatment cybersecurity end users" – U.S. subsidiaries (i.e., a foreign branch or most foreign subsidiaries of U.S. companies), financial services providers, insurance companies, and civil health and medical institutions providing medical treatment or research; (2) "vulnerability disclosure" or "cyber incident response; (3) Deemed exports
D:2	No government end-users	EXCEPTION: Can use ACE for some exports to Israel**
D:3	No government end-users	EXCEPTION: Can use ACE for some exports to Israel and Taiwan**
D:4	No government end-users	EXCEPTION: Can use ACE for some exports to Israel**

D:5	No government end-users; no non-government end-users	EXCEPTION: (1) Can use ACE for some exports to Cyprus;** (2) Exports, reexports or transfers (in-country) of ECCNs 4A005, 4D001.a (for 4A005 or 4D004), 4D004, 4E001.a (for 4A005), 4D001.a (for 4A005 or 4D004) to "favorable treatment cybersecurity end users" – U.S. subsidiaries (i.e., a foreign branch or most foreign subsidiaries of U.S. companies), financial services providers, insurance companies, and civil health and medical institutions providing medical treatment or research; (3) "vulnerability disclosure" or "cyber incident response;" (4) Deemed exports
E:1	Cannot use ACE	
E:2	Cannot use ACE	

** May use ACE for: (1) "digital artifacts" that are related to a cybersecurity incident involving information systems owned or operated by a "favorable treatment cybersecurity end user"; (2) exports to police or judicial bodies in Israel, Taiwan, and Cyprus for purposes of criminal or civil investigations or prosecutions of such cybersecurity incidents; (3) exports to national computer security incident response teams in Israel, Taiwan, and Cyprus of "cybersecurity items" for purposes of responding to cybersecurity incidents, for purposes of "vulnerability disclosure," or for purposes of criminal or civil investigations or prosecutions of such cybersecurity incidents.