



U.S. Department of Justice

National Security Division

Counterintelligence and Export Control Section

*950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530*

October 20, 2026

Eric S. Volkman
Latham & Watkins LLP
555 Eleventh Street, NW
Suite 1000
Washington, D.C. 20004

Re: Extreme Networks, Inc.

Dear Counsel:

The United States Department of Justice, National Security Division ("NSD"), Counterintelligence and Export Control Section and the United States Attorney's Office for the Eastern District of North Carolina (together, the "Offices") and Extreme Networks, Inc., a corporation formed under the laws of Delaware and headquartered in Morrisville, North Carolina (the "Company"), pursuant to the authority granted by its Board of Directors, enter into this Non-Prosecution Agreement ("Agreement").

1. On the understandings specified below, the Offices will not criminally prosecute the Company for any crimes relating to or arising from any of the conduct described in this Agreement or the Statement of Facts attached hereto as Attachment A ("Statement of Facts"). To the extent there is conduct disclosed by the Company that is not set forth in the attached Statement of Facts, such conduct will not be exempt from prosecution and is not within the scope of or relevant to this Agreement.

2. The Offices enter into this Non-Prosecution Agreement based on the individual facts and circumstances presented by this case and the Company, including:

(a) The nature and seriousness of the offense conduct, as described in the Statement of Facts, including that the Company indirectly (through a distributor) conducted business with a Russian weapons manufacturer that was owned by a party that was on the List of Specially Designated Nationals and Blocked Persons ("SDN List") at the time of the relevant conduct and concealed that business from the U.S. Government, which conduct harmed the national security of the United States by undermining the goals of the economic sanctions and export controls imposed by U.S. law; but also including the fact that the misconduct was committed by a small group of employees in the Company's Russia-based subsidiary (which was subsequently shut down) who actively concealed the activity from the Company's U.S.-based

compliance personnel after the Company acquired the Russian subsidiary from another company, and which misconduct yielded less than half a million dollars in sales revenue;

(b) The Company self-disclosed to the Offices the conduct that forms the basis for this Agreement; however, under the Department of Justice’s Corporate Enforcement and Voluntary Self-Disclosure Policy (“CEP”),¹ the disclosure was not timely as it was not “prior to an imminent threat that DOJ would learn of misconduct.” CEP, app. A. The Company learned of allegations regarding certain aspects of the possible misconduct by the Company’s Russia-based employees from a whistleblower report in April 2022, approximately 6 months prior to the Company’s self-disclosure to the Offices. In response, the Company conducted a good faith in-house investigation of those allegations, in consultation with outside counsel. Several months later the Company was informed of additional allegations and re-opened and expanded its internal investigation, which was in progress in October 2022 when the Company was contacted by an investigative journalist who, in a request for comment, cited new facts previously unknown to the Company’s counsel regarding the possibility of willful misconduct by the Company’s Russia-based employees. The Company quickly retained external counsel, disclosed the potential violation to NSD in a written voluntary self-disclosure which preceded the publication of the news article reported by the investigative journalist by a matter of days, and expanded its investigation. Although the Company’s self-disclosure does not meet the CEP’s standard for timeliness and voluntariness because it was submitted in anticipation of imminent public disclosure, the Offices give significant weight in determining the appropriate disposition of this matter to the circumstances surrounding the Company’s effort to learn of and disclose the misconduct, including the evidence demonstrating the Company’s good faith efforts to investigate earlier, incomplete allegations of misconduct;

(c) the Company received full credit for its cooperation with the Offices’ investigation, including credit for (i) timely responding to multiple subpoenas on a rolling basis yielding nearly 400,000 documents and providing translations of certain documents; (ii) voluntarily expanding the scope of its efforts to identify and produce additional responsive documents to the government; (iii) making current and former employees, including foreign-based employees, available for voluntary interview and securing pool counsel when requested by the interviewee; (iv) conducting an internal investigation and presenting its findings to the Offices; and (v) agreeing to toll the statute of limitations while the Offices pursued their investigation;

(d) the Company timely remediated by (i) terminating its Russian subsidiary and Russian-located personnel and terminating a distribution agreement with the distribution company involved in the unlawful sales; (ii) increasing the frequency of trade compliance training for customer-facing roles from biennially to annually; (iii) hiring a third party compliance consultant to do an assessment on the Company’s Global Trade Compliance group; (iv) improving screening procedures, which include the expansion of end-user diligence, screening parameters, and country holds; (v) hiring additional compliance personnel to reinforce its Global Trade Compliance function; (vi) adopting a new denied party screening tool and process which requires compliance personnel to document the reasons for terminating a

¹ Available at <https://www.justice.gov/dag/media/1430731/dl?inline>

compliance hold and which conducts daily rescreening of all counterparties in the Company's customer database; and (vii) implementing procedures for diligence in connection with mergers and acquisitions;

(e) the Company has committed to continuing its cooperation with regard to any investigation by the Offices as set forth in paragraph 6 below;

(f) the Company has agreed to pay a criminal fine of \$487,860.92 for sanctions and export control offenses described in the Statement of Facts;

(g) the Company has agreed to pay a forfeiture money judgment of \$487,860.92 representing the proceeds of the sanctions and export control offenses described in the Statement of Facts;

(h) the Company has agreed to pay \$1,529,685.00 in administrative penalties imposed by the United States Department of the Treasury, Office of Foreign Assets Control ("OFAC") for the sanctions violations; and

(i) based on the Company's remediation and the state of its compliance program, which has proven effective in practice, and the Company's commitments to maintain its compliance program as described in Attachment C and to report to the Offices on its compliance program as described in Attachment D, the Offices have determined that it is not necessary to require the appointment of an independent compliance monitor as part of this resolution.

3. Accordingly, after considering (a) through (i) in Paragraph 2 above, the Offices have determined that the appropriate resolution of this case is a non-prosecution agreement with the Company, payment of a reduced criminal monetary penalty based on the Company's good faith efforts and substantial compliance with the requirements of the CEP, and payment by the Company of \$487,860.92 in forfeiture. The total criminal penalty for the sanctions and export control offenses described in the Statement of Facts is \$975,721.84, which includes both the criminal fine and forfeiture.

4. The Company admits, accepts, and acknowledges that it is responsible under United States law for the acts of its officers, directors, employees, and agents as set forth in the Statement of Facts attached hereto as Attachment A and incorporated by reference into this Agreement, and that the facts described in Attachment A are true and accurate. The Company also admits, accepts, and acknowledges that the facts described in Attachment A constitute violations of law, specifically conspiracy to commit an offense against the United States and conspiracy to defraud the United States, in violation of Title 18, United States Code, Section 371, a willful violation of an order, regulation, and prohibition issued under the Export Control Reform Act ("ECRA"), 50 U.S.C. § 4819, a willful violation of an order, regulation, and prohibition issued under the International Emergency Economic Powers Act ("IEEPA"), in violation of Title 50, United States Code, Section 1705(a) and (c), knowingly filing false export information, Title 13, United States Code, Section 305; and smuggling, in violation of Title 18 United States Code, Section 554. The Company expressly agrees that it shall not, through present or future attorneys, officers, directors, employees, agents or any other person authorized

to speak for the Company make any public statement, in litigation or otherwise, contradicting the acceptance of responsibility by the Company set forth above or the facts described in the Statement of Facts attached hereto as Attachment A. The Company agrees that if it, or any of its direct or indirect subsidiaries, investors, or affiliates issues a press release or holds any press conference in connection with this Agreement, the Company shall first consult the Offices to determine (a) whether the text of the release or proposed statements at the press conference are true and accurate with respect to matters between the Offices and the Company; and (b) whether the Offices have any objection to the release. If any person described above makes a public statement outside of a press release or press conference – including, without limitation, in an interview or earnings call – that the Offices determine contradicts in whole or in part a statement contained in the Statement of Facts, the Offices shall so notify the Company, and the Company may avoid a breach of this Agreement by publicly repudiating such statement(s) within five business days after notification.

5. The Company's obligations under this Agreement shall have a term of three years from the date on which the Agreement is executed (the "Term"). The Company agrees, however, that, in the event the Offices determine, in their sole discretion, that the Company has knowingly violated any provision of this Agreement or has failed to completely perform or fulfill each of the Company's obligations under this Agreement, an extension or extensions of the Term may be imposed by the Offices, in their sole discretion, for up to a total additional time period of one year, without prejudice to the Offices' right to proceed as provided in the breach provisions of this Agreement below. Any extension of the Agreement extends all terms of this Agreement, including the terms of the reporting requirement in Attachment D, for an equivalent period. Conversely, in the event the Offices find, in their sole discretion, that there exists a change in circumstances sufficient to eliminate the need for the reporting requirement in Attachment D and that the other provisions of this Agreement have been satisfied, the Agreement may be terminated early.

6. The Company shall cooperate fully with the Offices in any and all matters relating to the conduct described in this Agreement and Attachment A and other conduct under investigation by the Offices at any time during the Term, subject to applicable law and regulations, including data privacy and national security laws, as well as valid claims of a privilege or protection (including the attorney-client privilege and work product protection), until the later of the date upon which all investigations and prosecutions arising out of such conduct are concluded, or the end of the Term. At the request of the Offices, the Company shall also cooperate fully with other domestic or foreign law enforcement and regulatory authorities and agencies in any investigation of the Company, or its affiliates, or any of its present or former officers, directors, employees, agents, and consultants, or any other party, in any and all matters relating to the conduct described in this Agreement and Attachment A and other conduct under investigation by the Offices at any time during the Term. The Company agrees that its cooperation shall include, but not be limited to, the following:

(a) The Company represents that it has truthfully disclosed all factual information with respect to its activities, those of its affiliates, and those of its present and former directors, officers, employees, agents, and consultants relating to the conduct described in this Agreement and the attached Statement of Facts and other conduct under investigation by the

Offices at any time about which the Company has any knowledge and that it shall promptly and truthfully disclose all factual information with respect to its activities, those of its parent company and affiliates, and those of its present and former directors, officers, employees, agents, and consultants, including any evidence or allegations and internal or external investigations, about which the Offices may inquire. This obligation of truthful disclosure includes, but is not limited to, the obligation of the Company to provide to the Offices, upon request, any document, record or other tangible evidence about which the Offices may inquire of the Company including evidence that is responsive to any requests made prior to the execution of this Agreement, but in no instance shall the Company be required to waive an applicable privilege or protection.

(b) Upon request of the Offices, the Company shall designate knowledgeable employees, agents, or attorneys to provide to the Offices the information and materials described above on behalf of the Company. It is further understood that the Company must at all times provide complete, truthful, and accurate information.

(c) The Company shall use its best efforts to make available for interviews or testimony, as requested by the Offices, present or former officers, directors, employees, agents, and consultants of the Company. This obligation includes, but is not limited to, sworn testimony before a federal grand jury or in federal trials, as well as interviews with domestic or foreign law enforcement and regulatory authorities. Cooperation shall include identification of witnesses who, to the knowledge of the Company, may have material, non-privileged information regarding the matters under investigation.

(d) With respect to any information, testimony, documents, records, or other tangible evidence provided to the Offices pursuant to this Agreement, the Company consents to any and all disclosures, subject to applicable law and regulations, to other governmental authorities, including United States authorities, of such materials as the Offices, in their sole discretion, shall deem appropriate.

7. In addition, during the Term, should the Company learn of credible evidence or credible allegations of conduct that may constitute a criminal violation of U.S. export control or sanctions laws by the Company or its personnel, including ECRA, IEEPA, and the Trading with the Enemy Act, the Company shall promptly report such evidence or allegations to the Offices. No later than thirty (30) days after the expiration of the Term of this Agreement, the Company, by the Chief Executive Officer of the Company and the Trade Compliance Manager of the Company, will certify to the Department, in the form of executing the document attached as Attachment E to this Agreement, that the Company has met its disclosure obligations pursuant to this Agreement. Such certification will be deemed a material statement and representation by the Company to the executive branch of the United States for purposes of 18 U.S.C. § 1001.

8. The Company represents that it has implemented and will continue to implement a compliance and ethics program that meets, at a minimum, the elements set forth in Attachment C, which is incorporated by reference into this Agreement. Such program must be designed to prevent and detect violations of U.S. export controls and sanctions laws and regulations throughout its operations, including those of its affiliates, agents, and joint ventures, and those of its contractors and subcontractors whose responsibilities include offering or selling the

Company's products or services to potentially sanctioned customers or jurisdictions. In addition, the Company agrees that it will report to the Offices annually during the Term of the Agreement regarding remediation and implementation of the compliance measures described in Attachment C. These reports will be prepared in accordance with Attachment D. Thirty (30) days prior to the expiration of the Term, the Company, by its Chief Executive Officer and Trade Compliance Manager, will certify to the best of the certifier's knowledge after reasonable inquiry to the Offices, in the form of executing the document attached as Attachment F to this Agreement, that the Company has met its compliance obligations pursuant to this Agreement.

9. In order to address any deficiencies in its internal controls, policies, and procedures, the Company represents that it has undertaken, and will continue to undertake in the future, in a manner consistent with all of its obligations under this Agreement, a review of its existing internal controls, policies, and procedures regarding compliance with U.S. export controls and sanctions laws and regulations, as well as other applicable laws and regulations concerning export controls and sanctions. Where necessary and appropriate, the Company agrees to modify its existing compliance program to ensure that it maintains a rigorous compliance program that incorporates relevant internal controls, as well as policies and procedures, designed to effectively detect and deter violations of U.S. export controls and sanctions laws and regulations. In addition, the Company agrees that it will report to the Offices annually during the Term of the Agreement regarding remediation and implementation of the compliance measures described in Attachment C. These reports will be prepared in accordance with Attachment D.

10. The Company agrees that, as a result of the Company's conduct, including the conduct set forth in the attached Statement of Facts, the Offices could institute a civil and/or criminal forfeiture action against certain funds held by the Company and that such funds would be forfeitable to the United States pursuant to Title 18, United States Code, Sections 981(a)(1)(C) and 982(a)(2) and Title 28, United States Code, Section 2461(c). The Company hereby admits that the facts set forth in the Statement of Facts establish that at least \$487,860.92, representing the proceeds traceable to the commission of the offenses, are forfeitable to the United States (the "Forfeiture Amount"). The Company releases any and all claims it may have to the Forfeiture Amount, agrees that the forfeiture of such funds may be accomplished either administratively or judicially at the Offices' election, and waives the requirements of any applicable laws, rules, regulations, or procedural requirements governing the forfeiture of assets, including notice of the forfeiture. If the Offices seek to forfeit the Forfeiture Amount judicially or administratively, the Company consents to entry of a final judgment of forfeiture or declaration of forfeiture directed to such funds; and the Company waives any right to assert Eighth Amendment claims or defenses and any defense it may have under Title 18, United States Code, Sections 981-984, including but not limited to notice, timeliness of notice, statute of limitations, and venue. The Company agrees to sign any additional documents necessary to complete forfeiture of the Forfeiture Amount. The Company also agrees that it shall not file any claims, petitions for remission, or any other assertion of ownership or request for return relating to the Forfeiture Amount, or any other action or motion seeking to collaterally attack the seizure, restraint, forfeiture, or conveyance of the Forfeiture Amount, nor shall it assist any others in filing any such claims, petitions, actions, or motions.

11. The Company agrees to pay a fine of \$487,860.92 to the United States Treasury. Pursuant to Title 18, United States Code, Section 3571(d), the maximum fine that may be imposed is twice the gross gain, or approximately \$975,721.84. The parties agree that the Company shall pay a fine to the United States in the amount of \$487,860.92 no later than ten business days after the Agreement is fully executed. This reflects a discount for the Company's cooperation and self-disclosure.

12. The Company agrees to pay the Forfeiture Amount of \$487,860.92 no later than ten business days after the Agreement is fully executed. The Company acknowledges that no tax deduction may be sought in connection with the payment of any part of this criminal monetary penalty or forfeiture amount. The Company shall not seek or accept directly or indirectly reimbursement or indemnification from any source with regard to the penalty or disgorgement amounts that the Company pays pursuant to this Agreement or any other agreement entered into with an enforcement authority or regulator concerning the facts set forth in Attachment A.

13. Any portion of the Forfeiture Amount that is paid is final and shall not be refunded should the Offices later determine that the Company has breached this Agreement and commence a prosecution against the Company. In the event of a breach of this Agreement and subsequent prosecution, the Offices are not limited to the Forfeiture Amount. The Offices agree that in the event of a subsequent breach and prosecution, they will recommend to the Court that the amounts already paid pursuant to this Agreement be offset against whatever forfeiture the Court shall impose as part of its judgment. The Company understands that such a recommendation will not be binding on the Court.

14. The Offices agree, except as provided herein, that they will not bring any criminal or civil case against the Company relating to or arising from any of the conduct described in this Agreement or the Statement of Facts, attached hereto as Attachment A. The Offices, however, may use any information related to the conduct described in the attached Statement of Facts against the Company: (a) in a prosecution for perjury or obstruction of justice; (b) in a prosecution for making a false statement; (c) in a prosecution or other proceeding relating to any crime of violence; or (d) in a prosecution or other proceeding relating to a violation of any provision of Title 26 of the United States Code. This Agreement does not provide any protection against prosecution for any future conduct by the Company. In addition, this Agreement does not provide any protection against prosecution of any individuals, regardless of their affiliation with the Company.

15. If, during the Term of this Agreement, the Company (a) commits any felony under U.S. federal law; (b) provides in connection with this Agreement deliberately false, incomplete, or misleading information, including in connection with its disclosure of information about individual culpability; (c) fails to cooperate as set forth in this Agreement; (d) fails to implement a compliance program as set forth in this Agreement and Attachment C; (e) commits any act that is a criminal violation of U.S. export control or sanctions laws or regulations; or (f) otherwise fails specifically to perform or to fulfill completely each of the Company's obligations under the Agreement, regardless of whether the Offices become aware of such a breach after the Term of the Agreement is complete, the Company shall thereafter be subject to prosecution for any federal criminal violation of which the Offices have knowledge, including, but not limited

to, the conduct described in the attached Statement of Facts, which may be pursued by the Offices in the U.S. District Court for the Eastern District of North Carolina or any other appropriate venue. Determination of whether the Company has breached the Agreement and whether to pursue prosecution of the Company shall be in the Offices' sole and good faith discretion. Any such prosecution may be premised on information provided by the Company or its personnel. Any such prosecution relating to the conduct described in the attached Statement of Facts or relating to conduct known to the Offices prior to the date on which this Agreement was signed that is not time-barred by the applicable statute of limitations on the date of the signing of this Agreement may be commenced against the Company, notwithstanding the expiration of the statute of limitations, between the signing of this Agreement and the expiration of the Term plus one year. Thus, by signing this Agreement, the Company agrees that the statute of limitations with respect to any such prosecution that is not time-barred on the date of the signing of this Agreement shall be tolled for the Term plus one year. In addition, the Company agrees that the statute of limitations as to any violation of federal law that occurs during the Term will be tolled from the date upon which the violation occurs until the earlier of the date upon which the Offices are made aware of the violation or the duration of the Term plus five years, and that this period shall be excluded from any calculation of time for purposes of the application of the statute of limitations.

16. In the event the Offices determine that the Company has breached this Agreement, the Offices agree to provide the Company with written notice prior to instituting any prosecution resulting from such breach. Within thirty (30) days of receipt of such notice, the Company shall have the opportunity to respond to the Offices in writing to explain the nature and circumstances of the breach, as well as the actions the Company has taken to address and remediate the situation, which the Offices shall consider in determining whether to pursue prosecution of the Company.

17. In the event that the Offices determine that the Company has breached this Agreement: (a) all statements made by or on behalf of the Company to the Offices or to the Court, including the attached Statement of Facts, and any testimony given by the Company before a grand jury, a court, or any tribunal, or at any legislative hearings, whether prior or subsequent to this Agreement, and any leads derived from such statements or testimony, shall be admissible in evidence in any and all criminal proceedings brought by the Offices against the Company; and (b) the Company shall not assert any claim under the United States Constitution, Rule 11(f) of the Federal Rules of Criminal Procedure, Rule 410 of the Federal Rules of Evidence, or any other federal rule that any such statements or testimony made by or on behalf of the Company prior or subsequent to this Agreement, or any leads derived therefrom, should be suppressed or are otherwise inadmissible. The decision whether conduct or statements of any current director, officer or employee, or any person acting on behalf of, or at the direction of, the Company, will be imputed to the Company for the purpose of determining whether the Company has violated any provision of this Agreement shall be in the sole discretion of the Offices.

18. Except as may otherwise be agreed by the parties in connection with a particular transaction, the Company agrees that in the event that, during the Term of the Agreement, it undertakes any change in corporate form, including if it sells, merges, or transfers a substantial portion of its business operations as they exist as of the date of this Agreement, whether such

sale is structured as a sale, asset sale, merger, transfer, or other change in corporate form, it shall include in any contract for sale, merger, transfer, or other change in corporate form a provision binding the purchaser, or any successor in interest thereto, to the obligations described in this Agreement.

19. Any purchaser or successor in interest must also agree in writing that the Offices' ability to determine a breach under this Agreement is applicable in full force to that entity. The Company agrees that the failure to include these provisions in the transaction will make any such transaction null and void. The Company shall provide notice to the Offices at least thirty (30) days prior to undertaking any such sale, merger, transfer, or other change in corporate form. The Offices shall notify the Company prior to such transaction (or series of transactions) if they determine that the transaction(s) will have the effect of circumventing or frustrating the enforcement purposes of this Agreement. In addition, if at any time during the Term of the Agreement the Company engages in a transaction(s) that has the effect of circumventing or frustrating the enforcement purposes of this Agreement, the Offices may deem it a breach of this Agreement pursuant to the breach provisions of this Agreement. Nothing herein shall restrict the Company from indemnifying (or otherwise holding harmless) the purchaser or successor in interest for penalties or other costs arising from any conduct that may have occurred prior to the date of the transaction, so long as such indemnification does not have the effect of circumventing or frustrating the enforcement purposes of this Agreement, as determined by the Offices.

20. This Agreement is binding on the Company and the Offices but specifically does not bind any other component of the Department of Justice, other federal agencies, or any state, local or foreign law enforcement or regulatory agencies, or any other authorities, although the Offices will bring the cooperation of the Company and its compliance with its other obligations under this Agreement to the attention of such agencies and authorities if requested to do so by the Company. This Agreement does not provide any protection against prosecution for any future conduct by the Company or any of its present or former parents or subsidiaries. In addition, this Agreement does not provide any protection against prosecution of any individuals, regardless of their affiliation with the Company or any of its present or former parents or subsidiaries.

21. It is further understood that the Company and the Offices may disclose this Agreement to the public.

22. Each party shall bear its own costs, attorney's fees, and expenses.

23. This Agreement sets forth all the terms of the agreement between the Company and the Offices. No amendments, modifications or additions to this Agreement shall be valid

unless they are in writing and signed by the Offices, the attorneys for the Company, and a duly authorized representative of the Company.

Sincerely,

CHRISTIAN J. NAUVEL
Acting Chief
Counterintelligence and Export Control Section
National Security Division

Date: 10/21/2026

By: Maria Fedor
Maria Fedor
Trial Attorney

W. ELLIS BOYLE
United States Attorney
Eastern District of North Carolina

Date: 10/21/2026

By: Adam Hulbig
Adam Hulbig
Assistant United States Attorney

AGREED AND CONSENTED TO:

Extreme Networks, Inc.

Date: October 20, 2026 | 10:04:01 PM PDT

By: Ed Meyercord
Edward (Ed) Meyercord III
Chief Executive Officer
Extreme Networks, Inc.

Date: October 21, 2026 | 5:15:52 AM PDT

By: Eric Volkman
Eric Volkman
Latham & Watkins LLP
Counsel for Extreme Networks, Inc.

ATTACHMENT A

STATEMENT OF FACTS

Relevant Entities and Individuals

1. Extreme Networks, Inc. (“Extreme”), a corporation formed under the laws of Delaware and headquartered in Morrisville, North Carolina, was at all times relevant to the conduct described in this Statement of Facts a publicly traded company that designs, develops, and manufactures network infrastructure equipment and software for network management, policy, analytics, security, and access control. Extreme operates globally, employing over 2,000 people worldwide. After the Americas, the EMEA region (Europe, Russia, Middle East, and Africa) was the second largest source of revenue for Extreme, representing approximately 36% to 43% of the company’s net revenues between 2018 and 2023.

2. Extreme Networks Rus LLC (“EN-Russia”) was one of Extreme’s EMEA operating subsidiaries, and consisted of a Moscow office with fewer than 15 employees, including account executives and systems engineers. As detailed below, Extreme acquired Russian networking business together with several other assets from a U.S. based company (“Company-1”), while Company-1 was undergoing a reorganization in bankruptcy proceedings. EN-Russia followed Extreme’s general business model of selling products indirectly to end users through a network of distributors and resellers. After Russia’s invasion of Ukraine in February 2022, Extreme ceased all business activities in Russia and shuttered its Moscow office.

3. Extreme’s Global Trade Compliance group (“GTC”) reviews sales occurring globally for compliance with export control laws and conducts the classification review for Extreme products.

4. JSC Concern VKO Almaz-Antey, also known as the Air Defense Concern Almaz-Antey (“Almaz-Antey”) is a Russia-based state-owned enterprise that designs, develops and manufactures anti-aircraft, anti-missile, and non-strategic missile defense systems. Almaz-Antey was initially sanctioned by the U.S. Department of the Treasury’s Office of Foreign Assets Control (“OFAC”) in July 2014 pursuant to E.O. 13661, and then again in January 2023 pursuant to E.O. 14024.

5. Moscow Machinery Building Plant Avangard, also known as MMZ Avangard, (“MMZA”) is located at Ul. Klary Tsetkin 33, Moscow, 125130, Russia. MMZA maintained a website at <http://mmzavangard.ru>, and according to the archived version of their website from May 28, 2016, MMZA was established in 1942 when the State Defense Committee of the USSR wanted to create a new enterprise to organize the serial production of M-11D aircraft engines. Since 2002, MMZA has been a subsidiary of “Almaz-Antey,” and until at least October 2022, was a primary producer of the S-300 and S-400 anti-aircraft missile systems used by the Russian army.

6. According to MMZA’s website as of May 28, 2016,¹ “in 2002, by decree of the President of the country, JSC “Concern Air Defense Almaz-Antey” was established, and the state enterprise “Moscow Machine-Building Plant ‘AVANGARD’ was transformed into an open joint-stock company by a decree of the Government of the Russian Federation and included in JSC ‘Concern Air Defense Almaz-Antey.’” The same webpage noted that “JSC MMZ AVANGARD is one of the key enterprises of the country’s military-industrial complex.”

¹ Available at <https://web.archive.org/web/20161004000023/http://mmzavangard.ru/2016/05/28/na-zashhite-mirnogo-neba-rossii/>

7. Dmitrovskiy Experimental Mechanical Plant (“DEMZ”) was the name of a Russian company that MMZA used to acquire products and services from Company-1 and, later, Extreme equipment. While EN-Russia employees described DEMZ in internal records and in communications with other Extreme employees as a business working on “components for Metalworking construction of country houses[,]” there was little evidence to support that DEMZ was operating in that fashion at the time of the relevant conduct.

8. “EN-Russia Employee 1,” an individual whose identity is known to the Offices and Extreme, was a Russia-based employee of Extreme and previously worked at Company-1. EN-Russia Employee 1 was the account manager for the purported DEMZ account both while at Company-1 and Extreme, prior to leaving Extreme in June 2020. EN-Russia Employee 1 indicated in an email to Extreme as he was being considered for a job at EN-Russia that he worked on the “Almaz-Antey and MMZA project” while at Company-1.

9. “EN-Russia Employee 2,” an individual whose identity is known to the Offices and Extreme, was a Russia-based systems engineering employee of Extreme. EN-Russia Employee 2 previously worked at Company-1.

10. “EN-Russia Employee 3,” an individual whose identity is known to the Offices and Extreme, was a Russia-based employee of Extreme, who provided sales support to the EN-Russia sales team.

11. “MMZA Employee 1,” an individual whose identity is known to the Offices and Extreme, was MMZA’s Head of Communications and was the named representative on all DEMZ purchases to Extreme.

12. “MMZA Employee 2,” an individual whose identity is known to the Offices and Extreme, was MMZA’s employee who sought technical support and assistance from EN-Russia.

Relevant Statutes and Regulations

Klein Conspiracy

13. Title 18, United States Code, Section 371, defines two types of conspiracies: (1) conspiracies to commit a specific federal offense, and (2) conspiracies to defraud the United States. A person violates the first clause of Section 371 (the “offense clause”) by conspiring or agreeing to engage in conduct that is prohibited by a federal criminal statute. A person violates the second clause of Section 371 (the “defraud clause”) by agreeing to defraud the United States or any agency thereof. This conspiracy is often referred to as a *Klein* conspiracy after the first decision to recognize it, which involved a conspiracy to obstruct the Internal Revenue Service. See *United States v. Klein*, 247 F.2d 908 (2d Cir. 1957). The following are the elements of a *Klein* conspiracy:

- (i) There was an agreement between two or more persons to defraud the United States by interfering with or obstructing one of its lawful governmental functions;
- (ii) The interference or obstruction was done by deceit, craft, trickery, or at least by dishonest means;
- (iii) Defendant was a part of the conspiracy; and
- (iv) There was an overt act, that is, one of the conspirators did some act for purposes of carrying out the conspiracy.

As discussed in detail below, one of the U.S. government’s lawful functions is to regulate and enforce export control laws.

International Emergency Economic Powers Act

14. Enacted in 1977, the International Emergency Economic Powers Act (IEEPA) gives the President certain powers, defined in 50 U.S.C. § 1702, to deal with any threats with respect to

which the President has declared a national emergency, and prescribes criminal penalties for violations. Section 1705 provides, in part, that “[i]t shall be unlawful for a person to violate, attempt to violate, conspire to violate, or cause a violation of any license, order, regulation, or prohibition issued under this chapter.” 50 U.S.C. § 1705(a).

15. Pursuant to his authority under IEEPA and the National Emergencies Act (50 U.S.C. §§ 1601 *et seq.*), in March 2014, President Barack Obama issued a series of executive orders (EO) in the wake of Russia’s invasion and annexation of the Crimea region of Ukraine. On March 6, 2014, the President issued EO 13660, declaring a national emergency to deal with the national security and foreign policy threats posed by the invasion. EO 13661 and EO 13662 were issued on March 16, 2014, and March 20, 2014, respectively, and expanded the scope of the initial emergency declaration. On December 19, 2014, the President issued EO 13685, which took additional steps to address the Russian occupation of Crimea. Together, these orders authorized the imposition of sanctions against persons responsible for or complicit in certain activities with respect to Ukraine; against officials of the Russian Federation; against persons operating in the arms or related material sector of the Russian Federation; and against individuals and entities operating in Crimea.

16. On July 16, 2014, pursuant to EO 13661, the U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC) added Almaz-Antey to the list of Specially Designated Nationals and Blocked Persons (SDN List). MMZA was not listed on the SDN List at the time of the relevant conduct, but was subsequently designated, pursuant to EO 14024, on June 28, 2022.

Export Control Reform Act

17. On August 13, 2018, President Donald Trump signed into law the National Defense Authorization Act of 2019, which included the Export Control Reform Act (ECRA). See 50 U.S.C. § 4801 et seq. ECRA provides permanent statutory authority for the Export Administration Regulations (EAR), 15 C.F.R. §§ 730-774, which most recently had been operative under IEEPA.

18. ECRA provides that “the national security and foreign policy of the United States require that the export, reexport, and in-country transfer of items, and specified activities of United States persons, wherever located, be controlled.” 50 U.S.C. § 4811. To that end, ECRA grants the President the authority to “(1) control the export, reexport, and in-country transfer of items subject to the jurisdiction of the United States, whether by United States persons or foreign persons; and (2) the activities of United States persons, wherever located, relating to” specific categories of items and information. 50 U.S.C. § 4812. ECRA grants to the Secretary of Commerce the authority to establish the applicable regulatory framework. 50 U.S.C. § 4813.

19. ECRA allows the Department of Commerce to review and control the export of certain items, including goods, software, and technologies. The EAR outline the regulatory framework as provided by ECRA. In particular, the EAR restrict the export of items that could contribute to the military potential of other nations or that could be detrimental to United States foreign policy or national security. The EAR impose licensing and other requirements for items subject to the EAR to be lawfully exported from the United States or lawfully reexported from one foreign destination to another.

20. Through the EAR, the Department of Commerce’s Bureau of Industry and Security (BIS) reviews and controls the export from the United States to foreign countries of certain U.S. items. Additionally, BIS has placed restrictions on the export and reexport of items that it has

determined could make a significant contribution to the military potential or nuclear proliferation of other nations or that could be detrimental to the foreign policy or national security of the United States. Under the EAR, such restrictions depend on several factors, including the technical characteristics of the item, the destination country, the end-user, and the end-use. The most sensitive items subject to EAR controls are identified on the Commerce Control List (CCL), set forth in 15 C.F.R. Part 774, Supplement Number 1. Items listed on the CCL are categorized by Export Control Classification Number (ECCN), each of which have export control requirements depending on destination, end-use, and end-user.

21. The Department of Commerce, through the U.S. Census Bureau, requires that for all exports valued over \$2,500 or for which an export license is required for shipment outside of the United States, the U.S. seller, manufacturer, exporter, or its shipping agent is required to file detailed information with the United States Government, which enables the government “to prevent the export of certain items to unauthorized destinations and/or end users.” 15 C.F.R. § 30.1(b). This information is submitted electronically by filing an electronic export information (EEI) via the Automated Export System (AES) with the United States government. EEI includes, among other things, detailed information about the seller, manufacturer, or exporter, the date of export, the ultimate end-user, the country of ultimate destination, the value of the goods being exported, the ECCN, and if applicable, the export license number.

22. By filing this information with the United States Government, the filer is certifying that the EEI information is true, accurate, and complete. 15 C.F.R. § 758.1(f). Knowingly providing false or misleading information, or causing such information to be provided, in connection with the preparation and submission of “export control documents,” including EEI filings, is a violation of the EAR and the Export Control Reform Act. 15 C.F.R. §764.2(g)(1)(ii),

IEEPA, 13 U.S.C. § 305, and 18 U.S.C. §1001; *see* 15 C.F.R. § 772.1 (EAR defines an “Export control document” to include, among other things, “EEI on the Automated Export System (AES) presented in connection with shipments to any country”). Similarly, concealing information from the Department of Commerce or U.S. Customs Service by failing to file EEI in connection with an export also violates the EAR, 13 U.S.C. § 305 and 18 U.S.C. § 1001(a)(1). *See* 15 C.F.R. § 764.2(g)(1).

23. Under the Foreign Trade Regulations, the exporter is required to identify in an EEI filing the ultimate consignee, i.e., the person who actually received the export in the foreign country, who is known to the exporter at the time of the product’s export from the United States. *See* 15 CFR 30.6(a)(3) (“**Ultimate consignee.** The ultimate consignee is the person, party, or designee that is located abroad and actually receives the export shipment. The name and address of the ultimate consignee, whether by sale in the United States or abroad or by consignment, shall be reported in the EEI. The ultimate consignee as known at the time of export shall be reported.”).

24. When sales are made to a distributor and the seller knows the identity of the distributor’s customer for a particular item, then the distributor is an intermediate consignee. *See* 15 CFR 30.6(b)(2) (“**Intermediate consignee...** The intermediate consignee acts in a foreign country as an agent for the principal party in interest or the ultimate consignee for the purpose of effecting delivery of the export shipment to the ultimate consignee.”)

25. In many cases, the identity of the ultimate consignee and ECCN determines whether the goods may be exported a) without any specific authorization from the United States government; b) with the specific authorization or a license from the United States Department of Commerce, the United States Department of State, or the United States Department of Treasury; or c) whether the goods may not be exported from the United States. Furthermore, accurate EEI

filings strengthen the United States government's ability to prevent the export of certain items to unauthorized destinations and end-users because the AES aids in targeting, identifying, and, when necessary, confiscating suspicious or illegal shipments prior to exportation. Without these EEIs being accurately filed, the U.S. government loses its ability to track shipments exiting the United States that may be destined for a prohibited end use or end user.

26. Title 50, United States Code, Section 4819(a)(2)(F), makes it a federal crime for any person to make any false or misleading representation, statement, or certification, or falsify or conceal any material fact, either directly to the Department of Commerce, or an official of any other U.S. agency, or indirectly through any other person in connection with the preparation, submission, issuance, use, or maintenance of any export control document or any report filed or required to be filed pursuant to the EAR.

The Criminal Scheme

27. Between around March 2018 and continuing through March 2022, in the Eastern District of North Carolina and elsewhere, Extreme, as a result of the actions of its employees and agents, including EN-Russia employees, conspired and agreed with others to defraud the United States and willfully violate U.S. sanctions and export controls by selling products and services ultimately intended for MMZA while misrepresenting the true end user on EEIs submitted to the U.S. government, which uses that data, as described above, to regulate whether certain exports should be authorized. Accordingly, the U.S. government was stripped of its ability to execute its lawful function of export control regulation aimed, in part, to protect national security and economic interests.

28. During this time, EN-Russia employees were acting within the scope of their employment, acted on behalf of Extreme, and for the benefit of Extreme. Moreover, pursuant to

Extreme's standard compliance procedures, EN-Russia's sales were approved by Extreme's GTC and order management, both headquartered in the U.S. Additionally, certain EN-Russia employees regularly engaged with Extreme's GTC and were aware of the oversight conducted by Extreme prior to all sales to Russian end users given the automatic compliance hold for all sales, at that time, to Russia.

29. Outside of routine engagement with GTC, multiple documents generated and handled by EN-Russia employees reinforced the requirement that their sales must abide by U.S. export laws. These notices were included, for example, in the Extreme Networks Terms and Conditions of Sales, the Discount Approval ("DA") forms, and the Distributor Agreements. GTC has also required that some customers, including the purported DEMZ customer, provide an End User Certificate, which further detailed the requirement that the sales not violate U.S. government export control laws. However, certain EN-Russia employees willfully concealed the true end user of the purported DEMZ sales which then caused Extreme to file false EEIs, where MMZA was not accurately identified as the end user. These false EEI filings thereby defrauded the United States of its ability to perform its lawful function to regulate U.S. exports.

Asset Purchase Agreement

30. On March 7, 2017, Extreme entered into an Asset Purchase Agreement ("APA") in which Extreme agreed to purchase the networking business of Company-1, which was then in Chapter 11 bankruptcy proceedings, for approximately \$100 million. The assets acquired by Extreme included Company-1's Russia-based customers. The completion of the acquisition of Company-1's Russian networking assets, however, was not concluded until March 2018.

31. Almaz-Antey, MMZA, and DEMZ were documented customers of Company-1 at different times prior to Extreme's acquisition. Company-1's last documented activity for Almaz-

Antey was a dead or lost opportunity for \$80,000 on April 12, 2017. On the same day, DEMZ made a purchase valued at \$80,000 from Company-1. Notably, the April 12, 2017 date that Company-1 listed for the dead or lost opportunity for Almaz-Antey post-dates when Almaz-Antey was first sanctioned by the U.S. Department of Treasury. In addition to customer accounts, Extreme also assumed several service orders from Company-1. One of these service orders was a February 13, 2018 service contract between Company-1 and a third-party distributor for three specific product types. The agreement lists MMZ “Avangard” of 33, Klary Cetkin str, Moscow 125130 as the end user.

32. Two EN-Russia employees previously worked at Company-1 before joining EN-Russia and worked with MMZA directly. One such employee, EN-Russia Employee 1, was the account manager for the purported DEMZ account while at Company-1 and also informed EN-Russia, prior to his hiring, that he previously worked on an MMZA project he referred to as “Almaz Antey (factories MMZ Avangard)[,]” which he further noted was a continuing project that was transferred to Extreme. Again, this representation of Almaz Antey continuing at Extreme post-dates when Almaz Antey was first sanctioned. EN-Russia Employee 1, by making this representation of the ongoing Almaz Antey – MMZA project, confirms that EN-Russia Employee 1 knew of the ownership structure between MMZA and Almaz Antey at the time the account was being transferred to EN-Russia.

33. Another employee who had formerly worked at Company-1 and engaged directly with MMZA was EN-Russia Employee 2. As noted below, prior to the first post-APA sale by Extreme, MMZA sought assistance for ongoing technical support and formulating the first post-APA sales order from EN-Russia Employee 2, who was then an employee of a distributor.

Extreme's Sales and Engagement with MMZA

34. In the months leading up to the first post-APA sale by Extreme to the DEMZ account name, Extreme employees engaged directly with MMZA personnel to both troubleshoot ongoing equipment issues and to formulate their next purchase order. During this time and throughout their relationship, when engaging directly with EN-Russia employees, MMZA did not conceal their identity from EN-Russia employees. Rather, MMZA employees used their mmza.ru email addresses and displayed signature blocks identifying their company as MMZA, in one instance also identifying the connection between MMZA and Almaz-Antey. For example, while working at a Russian distributor, EN-Russia Employee 2 provided direct support to MMZA employees at the request of another EN-Russia employee and assisted in the formulation of the first Extreme purchase order post APA. Additionally, EN-Russia employees visited MMZA on multiple occasions in connection with the support and services being provided by Extreme directly to MMZA.

35. While direct engagement between EN-Russia employees and MMZA employees was conspicuous, certain EN-Russia employees attempted to obfuscate the MMZA identity within Extreme's systems. For example, in February 2019, MMZA Employee 2, who was using his MMZA email address, asked EN-Russia Employee 2 about accessing the Extreme customer portal, which would give a customer the ability to submit service requests and download software. EN-Russia Employee 2 advised MMZA Employee 2 to fill in "DEMZ" in the "Company Name" field during the portal registration process. In March, MMZA Employee 2 applied for Extreme portal access by identifying the company as DEMZ. This initial request, which had some incomplete answers, was automatically denied, and GTC emailed MMZA Employee 2's provided MMZA email address asking that he complete the rest of the form to

include the user's full company name, address, and a corporate email. MMZA Employee 2 then resubmitted his portal access request and while providing the company name again as DEMZ, MMZA Employee 2 provided MMZA's address as the address for DEMZ. MMZA Employee 2 did not, however, conceal his MMZA email address in the resubmission. The compliance hold on this portal request was lifted later that day despite the company address resolving to MMZA and the email domain not matching the company's name.

36. Extreme's GTC did not question the connection between DEMZ and MMZA until December 2019, when an Order Management member asked the distributor about the connection between DEMZ and email domain mmza.ru – the domain name identified by the distributor in connection with the order - which is the same email domain that MMZA Employee 2 used to get his portal access approved in February 2019. Rather than answer the question about their customer to Extreme, the distributor forwarded the question posed by Order Management to two EN-Russia employees, one of whom was EN-Russia Employee 1. After receiving no response from EN-Russia, the distributor followed up again with EN-Russia Employee 1 in January 2020 asking how to respond about DEMZ. EN-Russia Employee 1 then forwarded the email to EN-Russia Employee 3 saying "We can somehow look/find out where this site address suddenly popped up. Who sent him first and how did it end up in the DA?! It can't be left here and apparently the DA needs to be redone[.]" Later in the day, the distributor emailed GTC claiming mmza.ru was the email domain and the order was ultimately approved.

37. In October 2020, Order Management asked the distributor for a link to DEMZ's online presence, and the distributor responded mmza.ru is the customer's email domain. When pushed by Order Management for an actual website address to ascertain their connection to military or sensitive company, the distributor responded that the "correct" website is ooodmz.ru.

While the distributor changed the purchase order to include the oodmz.ru email domain, the MMZA address remained in the purchase order as the address for DEMZ. Order Management forwarded the exchange with the distributor to GTC. After raising issues about the website mmza.ru and possible connections to a military contractor, GTC requested via Order Management an end user certification from DEMZ. The distributor submitted an end user certificate on purported DEMZ letterhead, which included an address that did not match the one on the purchase order. GTC failed to identify the apparent Russian-language discrepancies in the letterhead, which did not match the proper spelling of the purported end user (i.e., it translated as “Dmitrovsky Metallurgical Plant,” instead of “Dmitrovskiy Experimental Mechanical Plant”), but Order Management did ask the distributor about the address in the DEMZ end user certificate not matching the one in the purchase order, which listed the address for MMZA. While Extreme’s GTC failed to appropriately identify the various red flags associated with the purported DEMZ account, EN-Russia employees created sales to DEMZ without identifying MMZA as the ultimate end-user, which caused Extreme to file false EEIs.

38. Between September 2018 and May 2021, Extreme processed and fulfilled 9 revenue yielding purchase orders² for networking equipment and services from DEMZ, including transceivers, wireless ports, switches, and power supply units.³ Given that certain EN-Russia employees knew the identity of the “person, party, or designee that ... actually receives the export shipment,” Extreme was required to identify the ultimate consignee, MMZA, in their EEI filings. However, in all shipments made between September 2018 and May 2021, Extreme

² In total, Extreme fulfilled 11 purchase orders. However, two of these purchase orders yielded \$0 in revenue and were for the provision of software and cloud subscriptions.

³ In addition to these purchase orders, Extreme fulfilled eight repair and maintenance (“RMA”) transactions.

submitted EEIs that falsely identified either the distributor or DEMZ as the ultimate consignee. Accordingly, Extreme, through its employees and agents, including EN-Russia employees, knowingly and willfully filed false EEIs, which defrauded the U.S. government by interfering with the U.S. government's lawful function of export control regulation aimed, in part, to protect national security and economic interests.

39. Additionally, as noted above, the ownership relationship between MMZA and Almaz Antey should have been apparent from multiple sources, including MMZA Employee 1's signature block. The apparent ownership association between Almaz Antey and MMZA was reflected in EN-Russia Employee 1 promoting his prior work in the then-ongoing Almaz Antey – MMZA project that was transferred to Extreme and MMZA's mention of Almaz Antey in its now-archived website. Employees of EN-Russia attempted to conceal the true end user of the purported DEMZ sales in order to obfuscate the connection of DEMZ to MMZA, an entity owned by Almaz Antey, a sanctioned entity.

40. The total value of the products exported during this time frame was approximately \$487,860.92.

Discovery of Wrongdoing

41. In April 2022, Extreme received a whistleblower complaint of possible wrongdoings within EN-Russia. Extreme then conducted a good faith internal investigation, which included engagement with their outside counsel and presentation to the Board of Directors in the summer of 2022. In October 2022, a news outlet contacted Extreme regarding possible wrongdoings at EN-Russia and explicitly identified EN-Russia's business with MMZA. As a result of information provided by the news publication during this request for comments for a potential forthcoming news publication, Extreme expanded its internal investigation and

identified the email above from EN-Russia Employee 1 to EN-Russia Employee 3 regarding the DA. Additionally, Extreme identified evidence that EN-Russia engaged with MMZA at in-person meetings. Once Extreme uncovered this evidence, Extreme immediately notified the U.S. Department of Justice, the U.S. Department of Treasury, and the U.S. Department of Commerce. Extreme then performed an in-depth review of all of the Company's sales to Russia and Eastern Europe between July 2017 and November 2022, which it disclosed to the government.

ATTACHMENT B

CERTIFICATE OF BOARD APPROVAL

WHEREAS, Extreme Networks, Inc. (the “Company”) has been engaged in discussions with the United States Department of Justice, National Security Division, Counterintelligence and Export Control Section and the United States Attorney’s Office for the Eastern District of North Carolina (collectively, the “Offices”) regarding issues arising in relation to certain export control and sanctions violations committed by the Company;

WHEREAS, in order to resolve such discussions, it is proposed that the Company enter into a certain agreement with the Offices; and

WHEREAS, the Company’s Chief Executive Officer, Edward (Ed) Meyercord III, together with outside counsel for the Company, have advised the Board of Directors of the Company of its rights, possible defenses, the Sentencing Guidelines’ provisions, and the consequences of entering into such agreement with the Offices;

Therefore, the Board of Directors has APPROVED that:

1. The Company (a) enters into this non-prosecution agreement (“Agreement”) with the Offices; and (b) agrees to pay a Total Penalty of \$975,721.84, which includes a forfeiture of \$487,860.92 and fine of \$487,860.92. The Total Penalty will be paid to the United States in accordance with the terms of the Agreement and in the manner described in the Agreement;

2. The Company accepts the terms and conditions of this Agreement, including, but not limited to, (a) a knowing waiver for purposes of this Agreement and any charges by the United States arising out of the conduct described in the attached Statement of Facts of any objection with respect to venue in the United States District Court for the Eastern

District of North Carolina; and (b) a knowing waiver of any defenses based on the statute of limitations for any prosecution relating to the conduct described in the attached Statement of Facts or relating to conduct known to the Offices prior to the date on which this Agreement was signed that is not time-barred by the applicable statute of limitations on the date of the signing of this Agreement;

3. The Chief Executive Officer of the Company, Edward (Ed) Meyercord III, is authorized, empowered, and directed, on behalf of the Company to execute the Agreement substantially in such form as reviewed by the Board of Directors at a meeting held on October 15, 2026, with such changes as the Chief Executive Officer of the Company, Edward (Ed) Meyercord III, may approve;

4. The Chief Executive Officer of the Company, Edward (Ed) Meyer cord, is authorized, empowered and directed to take any and all actions as may be necessary or appropriate and to approve the forms, terms or provisions of any agreement or other documents as may be necessary or appropriate, to carry out and effectuate the purpose and intent of the foregoing approval; and

5. All of the actions of the Chief Executive Officer of the Company, Edward (Ed) Meyercord III, which actions were authorized by the approval, are severally ratified, confirmed, approved, and adopted as actions on behalf of the Company.

By: Ed Meyercord
Edward (Ed) Meyercord, CEO
Extreme Networks, Inc.

October 20, 2026 | 10:04:01 PM PDT

Date

ATTACHMENT C

CORPORATE COMPLIANCE PROGRAM

In order to address any deficiencies in its internal controls, compliance code, policies, and procedures regarding compliance with the International Emergency Economic Powers Act (“IEEPA”), 50 U.S.C. §§ 1705 *et seq.*, the Export Control Reform Act (“ECRA”), 50 U.S.C. §§ 4801 *et seq.*, and other applicable export control and sanctions laws, Extreme Networks, Inc. (the “Company”) agrees to continue to conduct, in a manner consistent with all of its obligations under this Agreement, appropriate reviews of its existing internal controls, policies, and procedures.

Where necessary and appropriate, the Company agrees to modify its compliance program, including internal controls, compliance policies, and procedures in order to ensure that it maintains an effective and risk-based export control and sanctions compliance program, consistent with the Company’s risk profile, size, and complexity, that incorporates relevant policies and procedures designed to effectively detect and deter violations of IEEPA, ECRA, and other applicable export control and sanctions laws and regulations. At a minimum, this should include, but not be limited to, the following elements to the extent they are not already part of the Company’s existing internal controls, compliance code, policies, and procedures:

Commitment to Compliance

1. The Company will ensure that its directors and senior management continue to provide strong, explicit, and visible support and commitment to compliance with its corporate policy against violations of export control and sanctions laws, its compliance policies, and its Code of Conduct, and demonstrate rigorous support for compliance principles via their actions and words.

2. The Company will continue to ensure that mid-level management throughout its organization reinforce leadership's commitment to compliance policies and principles and encourage employees to abide by them. The Company will maintain a culture of ethics and compliance with the law in their day-to-day operations at all levels of the Company.

Periodic Risk Assessment and Review

3. The Company will maintain a risk management process to identify, analyze, and address the individual circumstances of the Company, in particular the export control and sanctions risks facing the Company.

4. On the basis of its periodic risk assessment, the Company shall take appropriate steps to design, implement, or modify each element of its compliance program to reduce the risk of violations of the export control and sanctions laws, its compliance policies, and its Code of Conduct.

Policies and Procedures

5. The Company will maintain a clearly articulated and visible corporate policy against violations of IEEPA, ECRA, and other applicable export control and sanctions laws (collectively, the "export control and sanctions laws"), which shall be memorialized in a written compliance policy or policies.

6. The Company will maintain compliance policies and procedures designed to reduce the prospect of violations of the export control and sanctions laws and the Company's compliance policies and Code of Conduct, and the Company will continue to take appropriate measures to encourage and support the observance of ethics and compliance policies and procedures against violations of the export control and sanctions laws by personnel at all levels of the Company. These export control and sanctions law policies and procedures shall apply to all directors, officers,

and employees and, where necessary and appropriate, outside parties acting on behalf of the Company in a foreign jurisdiction, including all agents and business partners. The Company shall notify all employees that compliance with the policies and procedures is the duty of individuals at all levels of the Company. Such policies and procedures shall address, as applicable to the Company's business:

- a. Customer due diligence, including sanctions list screening;
- b. End user certificates;
- c. Applicability of U.S. sanctions laws and regulations to overseas activities;
- d. Compliance responsibilities of sales agents;
- e. High-risk jurisdictions; and
- f. Export control and sanctions compliance language in business contracts.

7. The Company shall review its export control and sanctions compliance policies and procedures as necessary to address changing and emerging risks and update them as appropriate to ensure their continued effectiveness, taking into account relevant developments in the field and evolving international and industry standards.

Independent, Autonomous, and Empowered Oversight

8. The Company will continue to maintain assignment of responsibility to one or more senior corporate executives of the Company for the implementation and oversight of the Company's export control and sanctions compliance policies and procedures. Such corporate official(s) shall have the authority to report directly to independent monitoring bodies, including internal audit, the Company's Board of Directors, or any appropriate committee of the Company's Board of Directors, and shall have an adequate level of autonomy from management as well as sufficient resources, authority, and support from senior leadership to maintain such autonomy.

Training and Guidance

9. The Company will maintain mechanisms designed to ensure that its Code of Conduct and export control and sanctions compliance policies and procedures are effectively communicated to all directors, officers, employees, and, where necessary and appropriate, agents and business partners. These mechanisms shall include: (a) periodic training for all directors and officers, all employees in positions of leadership or trust, positions that require such training (e.g., internal audit, sales, legal, compliance, finance), or positions that otherwise pose an export control or sanctions risk to the Company, and, where necessary and appropriate, agents and business partners; and (b) metrics for measuring knowledge retention and effectiveness of the training. The Company will continue to conduct training in a manner tailored to the audience's size, sophistication, or subject matter expertise and, where appropriate, will discuss prior compliance incidents.

10. The Company will maintain, or where necessary establish, an effective system for providing guidance and advice to directors, officers, employees, and, where necessary and appropriate, agents and business partners, on complying with the Company's export control and sanctions compliance policies and procedures, including when they need advice on an urgent basis or in any foreign jurisdiction in which the Company operates.

Confidential Reporting Structure and Investigation of Misconduct

11. The Company will maintain, or where necessary establish, an effective system for internal and, where possible, confidential reporting by, and protection of, directors, officers, employees, and, where appropriate, agents and business partners concerning violations of the

export control and sanctions laws or the Company's Code of Conduct or export control and sanctions compliance policies and procedures.

12. The Company will maintain, or where necessary establish, an effective and reliable process with sufficient resources for responding to, investigating, and documenting allegations of violations of the export control and sanctions laws or the Company's export control and sanctions compliance policies and procedures.

Compensation Structures and Consequence Management

13. The Company will maintain, or where necessary establish, clear mechanisms to incentivize behavior amongst all directors, officers, employees, and, where necessary and appropriate, parties acting on behalf of the Company that comply with its corporate policy against violations of the export control and sanctions laws, its compliance policies, and its Code of Conduct. These incentives shall include, but shall not be limited to, the implementation of criteria related to compliance in the Company's compensation and bonus system subject to local labor laws.

14. The Company will maintain, or where necessary establish, appropriate disciplinary procedures to address, among other things, violations of the export control and sanctions laws and the Company's Code of Conduct and export control and sanctions compliance policies and procedures by the Company's directors, officers, and employees. Such procedures should be applied consistently and fairly, regardless of the position held by, or perceived importance of, the director, officer, or employee. The Company shall maintain, or where necessary establish, procedures to ensure that where misconduct is discovered, reasonable steps are taken to remedy the harm resulting from such misconduct, and to ensure that appropriate steps are taken to prevent further similar misconduct, including assessing the internal controls, Code of Conduct, and

compliance policies and procedures and making modifications necessary to ensure the overall export control and sanctions compliance program is effective.

Third-Party Management

15. The Company will maintain appropriate risk-based due diligence and compliance requirements pertaining to the retention and oversight of all agents and business partners, including:

- a. properly documented due diligence pertaining to the hiring and appropriate and regular oversight of agents and business partners;
- b. informing agents and business partners of the Company's commitment to abiding by export control and sanctions laws, and of the Company's Code of Conduct and export control and sanctions compliance policies and procedures; and
- c. seeking a reciprocal commitment from agents and business partners.

16. The Company will, as appropriate, continue to engage in ongoing monitoring and risk management of third-party relationships through due diligence, training, audits, and/or annual compliance certifications by the third party.

17. Where necessary and appropriate, the Company will continue to include standard provisions in agreements, contracts, and renewals thereof with all agents and business partners that are reasonably calculated to prevent violations of the export control and sanctions laws, which may, depending upon the circumstances, include: (a) export control and sanctions representations and undertakings relating to compliance with the export control and sanctions laws; and (b) rights to terminate an agent or business partner as a result of any breach of the export control and sanctions laws, the Company's Code of Conduct or compliance policies, or procedures, or the representations and undertakings related to such matters.

Mergers and Acquisitions

18. The Company will maintain policies and procedures for mergers and acquisitions requiring that the Company conduct appropriate risk-based due diligence on potential new business entities, including appropriate export control and sanctions due diligence by legal, accounting, and compliance personnel.

19. The Company will ensure that the Company's Code of Conduct and compliance policies and procedures regarding the export control and sanctions laws apply as quickly as is practicable to newly acquired businesses or entities merged with the Company and will promptly:

a. train the directors, officers, employees, agents, and business partners consistent with Paragraphs 9-10 above on the export control and sanctions laws and the Company's compliance policies and procedures regarding export control and sanctions laws; and

b. where warranted, conduct a U.S. export control and sanctions-specific review of all newly acquired or merged businesses as quickly as practicable.

Monitoring and Testing

20. The Company will continue to conduct periodic reviews and testing of all elements of its compliance program to evaluate and improve their effectiveness in preventing and detecting violations of export control and sanctions laws and the Company's Code of Conduct and export control and sanctions compliance policies and procedures, taking into account the Company's risk profile, relevant developments in the field and evolving international and industry standards.

21. The Company will ensure that compliance and control personnel have sufficient direct or indirect access to relevant sources of data to allow for timely and effective monitoring and/or testing of transactions.

Analysis and Remediation of Misconduct

22. The Company will continue to conduct a root cause analysis of misconduct, to identify any systemic issues and/or any control failures. The Company will timely and appropriately remediate the root causes of misconduct. The Company will ensure that root causes, including systemic issues and controls failures, and relevant remediation are shared with management as appropriate.

ATTACHMENT D

REPORTING REQUIREMENTS

Extreme Networks, Inc. (the “Company”) agrees to report to the Counterintelligence and Export Control Section of the National Security Division of the U.S. Department of Justice (“NSD-CES”) and the United States Attorney’s Office for the Eastern District of North Carolina (“the Office”) periodically, at no less than twelve-month intervals during a three-year term, regarding remediation and implementation of the compliance program and internal controls, policies and procedures described in Attachment C. During this three-year term, the Company shall: (1) conduct an initial review and submit an initial report, and (2) conduct and prepare at least two follow-up reviews and reports, as described below:

1. By no later than one year from the date this Agreement is executed, the Company shall submit to NSD-CES and the Office a written report setting forth a complete description of its remediation efforts to date, its proposals reasonably designed to improve its internal controls, policies, and procedures for ensuring compliance with the International Emergency Economic Powers Act (“IEEPA”), 50 U.S.C. §§ 1705 *et seq.*; the Export Control Reform Act (“ECRA”), 50 U.S.C. §§ 4801 *et seq.*; and other applicable export control and sanctions laws, and the proposed scope of the subsequent reviews. The report shall be transmitted to the Chief of NSD-CES, U.S. Department of Justice, 950 Pennsylvania Avenue, N.W., Washington, D.C. 20530, and the United States Attorney for the Eastern District of North Carolina, 150 Fayetteville Street, Suite 2100, Raleigh, North Carolina 27601. The Company may extend the period for issuance of the report with prior written approval of NSD-CES and the Office.

2. The Company shall undertake at least two follow-up reviews and reports incorporating NSD-CES's and the Office's views on the Company's prior reviews and reports, to further monitor and assess whether the Company's policies and procedures are reasonably designed to detect and prevent violations of IEEPA, ECRA, and other applicable export control and sanctions laws.

3. The first follow-up review and report shall be completed by no later than one year after the initial report is submitted to NSD-CES and the Office. The second follow-up review and report shall be completed and delivered to NSD-CES and the Office no later than thirty days before the end of the three-year term described in Paragraph 1.

4. The reports will likely include proprietary, financial, confidential and competitive business information. Moreover, public disclosure of the reports could discourage cooperation, impede pending or potential government investigations and thus undermine the objectives of the reporting requirement. For these reasons, among others, the reports and the contents thereof are intended to remain and shall remain non-public, except as otherwise agreed to by the parties in writing, or except to the extent that NSD-CES and the Office determine in their sole discretion that disclosure would be in furtherance of NSD-CES's and the Office's discharge of their duties and responsibilities or is otherwise required by law.

5. The Company may extend the period for submission of any of the follow-up reports with prior written approval of NSD-CES and the Office.