OFFICE OF THE ATTORNEY GENERAL
STATE OF FLORIDA
DEPARTMENT OF LEGAL AFFAIRS

CONSUMER PROTECTION
SUBPOENA DUCES TECUM

IN THE INVESTIGATION OF: **TP-Link Systems Inc.**
AG CASE NO: L25-3-1099

TO: **TP-Link Systems Inc.**
c/o Registered Agent
C T Corporation System
330 N Brand Blvd Ste # 700
Glendale, CA 91203

THIS INVESTIGATIVE SUBPOENA DUCES TECUM is issued pursuant to the Florida Deceptive and Unfair Trade Practices Act, Chapter 501, Part II, Florida Statutes, in the course and authority of an official investigation. Your attention is directed to Sections 501.204, and 501.206, Florida Statutes, printed and attached hereto.

YOU ARE HEREBY COMMANDED to produce all documentary material and other tangible evidence as described herein, that is in your possession, custody, or control, or in the possession, custody, or control of your agents or employees, and to make it available for inspection and copying or reproduction before Senior Assistant Attorney General Henry Johnson and/or other Assistant Attorney(s) General on December 16, 2025 at 10 a.m. at the following location:

OFFICE OF THE ATTORNEY GENERAL
CONSUMER PROTECTION DIVISION
110 SE 6th Street, 10th Floor
Ft. Lauderdale, FL 33301

ALTERNATIVELY, this subpoena may be complied with by delivering copies of all of the requested materials, prior to the date set forth above to c/o Senior Assistant Attorney General Henry Johnson. The production of material in response to this demand shall include the following:

SEE ATTACHED ADDENDUM

WITNESS, the Department of Legal Affairs at Fort Lauderdale, Florida, this 2nd day of December, 2025.

JAMES UTHMEIER
ATTORNEY GENERAL

/s/Henry Q. Johnson
Henry Q. Johnson, CIPP/US
Senior Assistant Attorney General
Multistate and Privacy Bureau
Office of the Attorney General
110 SE 6th Street, 10th Floor
Ft. Lauderdale, FL 33301
Tel.: (954) 712-4600

501.204 Unlawful acts and practices.—
(1) Unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful.
(2) It is the intent of the Legislature that, in construing subsection (1), due consideration and great weight shall be given to the interpretations of the Federal Trade Commission and the federal courts relating to s. 5(a)(1) of the Federal Trade Commission Act, 15 U.S.C. s. 45(a)(1) as of July 1, 2017.

501.206 Investigative powers of enforcing authority.—
(1) If, by his or her own inquiry or as a result of complaints, the enforcing authority has reason to believe that a person has engaged in, or is engaging in, an act or practice that violates this part, he or she may administer oaths and affirmations, subpoena witnesses or matter, and collect evidence. Within 5 days, excluding weekends and legal holidays, after the service of a subpoena or at any time before the return date specified therein, whichever is longer, the party served may file in the circuit court in the county in which he or she resides or in which he or she transacts business and serve upon the enforcing authority a petition for an order modifying or setting aside the subpoena. The petitioner may raise any objection or privilege which would be available under this chapter or upon service of such subpoena in a civil action. The subpoena shall inform the party served of his or her rights under this subsection.
(2) If matter that the enforcing authority seeks to obtain by subpoena is located outside the state, the person subpoenaed may make it available to the enforcing authority or his or her representative to examine the matter at the place where it is located. The enforcing authority may designate representatives, including officials of the state in which the matter is located, to inspect the matter on his or her behalf, and he or she may respond to similar requests from officials of other states.
(3) Upon failure of a person without lawful excuse to obey a subpoena and upon reasonable notice to all persons affected, the enforcing authority may apply to the circuit court for an order compelling compliance.
(4) The enforcing authority may request that an individual who refuses to comply with a subpoena on the ground that testimony or matter may incriminate him or her be ordered by the court to provide the testimony or matter. Except in a prosecution for perjury, an individual who complies with a court order to provide testimony or matter after asserting a privilege against self-incrimination to which he or she is entitled by law shall not have the testimony or matter so provided, or evidence derived therefrom, received against him or her in any criminal investigation or proceeding.
(5) Any person upon whom a subpoena is served pursuant to this section shall comply with the terms thereof unless otherwise provided by order of the court. Any person who fails to appear with the intent to avoid, evade, or prevent compliance in whole or in part with any investigation under this part or who removes from any place, conceals, withholds, mutilates, alters, or destroys, or by any other means falsifies any documentary material in the possession, custody, or control of any person subject to any such subpoena, or knowingly conceals any relevant information with the intent to avoid, evade, or prevent compliance shall be liable for a civil penalty of not more than $5,000, reasonable attorney’s fees, and costs.

ADDENDUM

Definitions

A. "Agreement(s)" means any oral or written contract, arrangement, or understanding, whether formal or informal, between two or more persons, together with all modifications or amendments thereto.

B. "Company" or "companies" as used herein means the addressee/recipients of this subpoena, their parents, branches, departments, divisions, affiliates, subsidiaries, retail outlets, stores, franchises, successors, or predecessors, whether wholly owned or not, including, without limitation, any organization or entity in which said addressees have a management or controlling interest, together with all present and former officers, directors, agents, employees, sales people, brokers, representatives or anyone else acting or purporting to act, on behalf of the above-identified persons or entities, or through which TP-Link Systems Inc. ("TP-Link") may have conducted business. The term "you" and "your" shall be synonymous with "Company."

C. "Document" or "documents" as used herein shall include all paper records and all electronically stored information, including the original and any non-identical copy (whether different from the original because of notations on such copy or otherwise, and including all draft versions of the original), of any written, recorded, or graphic matter, however produced or reproduced, including, but not limited to, all correspondence, communications (as defined below in Paragraph G), web pages, social media communications, photographs, contracts (including drafts, proposals, and any and all exhibits thereto), drafts, minutes and agendas, memoranda (including inter and intra-office memoranda, memoranda for file, pencil jottings, diary entries, desk calendar entries, reported recollections, and any other written form of notation of events or intentions), transcripts and recordings of conversations and telephone calls, audio and video media files, books of account, ledgers, publications, professional journals, invoices, financial statements, purchase orders, receipts, canceled checks and all other paper or electronic documentary material of any nature whatsoever, together with any attachments thereto or enclosures therewith.

D. The term "any" shall be construed as synonymous with "all" and shall be all inclusive.

E. The connectives "and" and "or" shall be construed either disjunctively or conjunctively, whichever makes the request more inclusive.

F. "CISA" means the U.S. Cybersecurity and Infrastructure Security Agency.

G. "Communication" or "communications" means any act, action, oral speech, testimony, written correspondence, contact, expression of words, thoughts, or ideas, or transmission or exchange of data

or other information to another person, whether orally, person to person, in a group, by telephone, letter, personal delivery, intercom, fax, e-mail, text message, social media, or any other process, electric, electronic or otherwise in any medium. All such communications in writing shall include, without limitation, printed, typed, handwritten, or other readable documents.

H. "Person" means any individual and all entities, and, without limiting the generality of the foregoing, includes natural persons, employees, contractors, agents, consultants, vendors, telemarketers, consumers, customers, officers, directors, successors, assigns, joint owners, associations, partnerships, companies, joint ventures, corporations, affiliates, trusts, trustees, escrow agents and estates, and all groups or associations of persons.

I. "Related to" or "relating to" means in whole or in part constituting, containing, concerning, embodying, reflecting, discussing, describing, analyzing, identifying, stating, referring to, setting forth, dealing with, or in any way pertaining to.

J. "TP-Link networking product(s)" means all networking devices, including hardware, firmware, and other software, sold, distributed, or licensed by you.

Instructions

K. This Subpoena is for the production of all responsive documents and information in your possession, custody or control regardless of whether such documents or information is possessed directly by you or your directors, officers, agents, employees, representatives, subsidiaries, managing agents, affiliates, investigators, or by your attorneys or their agents, employees, representatives, or investigators.

L. Unless otherwise specified, original documents must be produced, and the originals of electronic files must be produced in accordance with Paragraph S herein. If your "original" is a photocopy, then the photocopy would be and should be produced as the original. Said copy shall be legible and bound or stapled in the same manner as the original.

M. The documents to be produced pursuant to each request should be segregated and specifically identified to indicate clearly the particular numbered request to which they are responsive.

N. If any responsive document or information cannot be produced in full, you are to produce it to the extent possible, indicating which document, or portion of that document, is being withheld, and the reason that document is being withheld.

O. If a document once existed and has subsequently been lost, destroyed, or is otherwise missing, please provide sufficient information to identify the document and state the details concerning its loss or destruction.

P. Documents not otherwise responsive to this Subpoena shall be produced if such documents mention, discuss, refer to, or explain the documents that are called for by this Subpoena, or if such documents are attached to documents called for by this Subpoena and constitute routing slips, transmittal memoranda, or letters, comments, evaluations, or similar materials.

Q. If you do not possess, control, or have custody of any documents responsive to any numbered request set forth below, state this fact by so specifying in your response to said request.

R. The use of the singular form of a word includes the plural and vice versa. In addition, the use of any tense of any verb includes all other tenses of the verb.

S. ***Electronically Stored Information*** (ESI) is to be produced in the form in which it is ordinarily maintained. For example, native files would include email, spreadsheets and word processing files. Responsive documents that exist in electronic format shall be provided in native format (e.g., Microsoft Word files (.doc) or Outlook (.pst), emails, spreadsheets and word processing documents) with standard metadata intact, as outlined below. Prior to any production of responsive data from a structured database (e.g., Oracle, SAP, SQL, MySQL, QuickBooks, etc.), the producing party shall first provide the database dictionary and a list of all reports that can be generated from the structured database. The list of reports shall be provided in native Excel (.xls) format. The database format will be requested for production after both parties agree on the format. Please include sufficient identification of the applicable software program to permit access to, and use of, each document. All attachments

must be linked to their electronic documents. Native files should be provided in directories which are identifiable as responsive to a specific document request. All documents produced in native form should be produced on CDROM, DVDROM, External USB, or other similar drive media of a type that can be read by any standard computer. Unless otherwise agreed to, standard metadata in electronically stored information shall be preserved and produced, such as: Custodian, To, From, CC, BCC, Dates and Times (Sent, Received and Modified), Attachments, Links and Document types. A more complete list can be provided upon request. Questions regarding electronic production should be directed to the Assistant Attorney General whose name appears on this Subpoena. Arrangements will be made for the communication with the appropriate in-house technical expert.

T. If you claim the attorney-client privilege, work-product privilege, or any other privilege, for any document, provide a detailed privilege log that contains at least the following information for each document that you have withheld:

1) The name of each author, writer, sender or initiator of such document or thing, if any;
2) The name of each recipient, addressee or party for whom such document or thing was intended, if any;
3) The date of such document, if any, or an estimate thereof so indicated if no date appears on the document;
4) The general subject-matter as described on such document; if no such description appears, then such other description sufficient to identify said document; and,
5) The claimed grounds for withholding the document, including, but not limited to, the nature of any claimed privilege and grounds in support thereof.

U. TRADE SECRET PROTECTION. In the event you seek to assert trade secret protection under Florida Statutes section 119.0715, or other applicable Florida Statutes, for each document for which trade secret protection is claimed:

1) Provide prior to, or simultaneous with, production of the document at issue, a sworn affidavit from a person with knowledge as to the basis for the trade secret claim, which complies with the following requirements:

a. The affidavit should specify the bates range of the claimed trade secret documents at issue, generally describe the documents at issue, and provide evidence of the application of the trade secret exemption.

b. The affidavit should attach a certification (similar in form to a traditional privilege log) that identifies the following information for each separate claimed trade secret document: (i) the bates range of the document; (ii) a description of the document sufficient to determine the application of the trade secret exemption; and (iii) the specific element(s) or provision(s) of section 688.002 that render the document at issue a trade secret exempted from public records.

2) Segregate and separately label the documents claimed as trade secrets as follows:

   a. Documents produced electronically should be produced on separate CD or electronic media clearly labeled "Trade Secret" on the physical media as well in the title of the electronic folder or file;

   b. Documents produced in hard copy should be separated and each clearly labeled "Trade Secret."

3) Any challenge to the application of the trade secret exemption shall be rebutted, if at all, only by you and not by the Office of the Attorney General, whose involvement shall be limited solely to providing notice to you of any challenge to your claim of trade secret protection. To the extent you seek to assert a trade secret exemption in connection with a public records request to the Office of the Attorney General, you shall be obligated to seek an appropriate protective order or otherwise establish the applicability of the trade secret claim and exemption. Failure to do so shall render the documents subject to production under any applicable public records requirements and not protected by a trade secret claim.

V. All document destruction or retention policies and practices and electronic file deletion or disk management policies and practices (including, but not limited to, reformatting practices) that could have the effect of altering or deleting information requested by this Subpoena should be suspended.

1) Because electronically stored information is an important and irreplaceable source of evidence, you must take appropriate steps to preserve all potentially relevant documents within your control or practical ability to access, which includes, but is not limited to, preserving information from computer systems, removable or portable electronic media (like CDs/DVDs, USB drives), e-mail, text/instant messaging, "tweets" and other electronic correspondence at work and other locations, word processing documents, spreadsheets, databases, calendars, telephone logs, cell phones, voicemail, blogs, social media, internet usage files, website data, personal computers/laptops, personal data assistants (PDAs), servers, and archives/backup files, as well as other tangible documentation that will be relevant to the discovery of admissible evidence in this matter, so as to avoid any potential claims for spoliation of evidence. This request pertains not only to documents that are directly responsive to this Subpoena, but to all other documents that relate to the subject of our investigation as well.

2) Preservation of electronic data in its native format is essential, as a paper printout of text contained in a computer file does not completely reflect all information contained within an electronic file. Additionally, due to its format, electronic evidence can be easily altered, deleted, corrupted or otherwise modified. Accordingly, you are required to take every reasonable step to preserve this information until the resolution of this matter. This includes, but is not limited to, the following obligations:

   a) Discontinue all data destruction and overwriting/recycling processes of relevant data;

   b) Preserve passwords, decryption procedures (and accompanying software), access codes, ID

codes, etc.; and

c) Maintain all pertinent information and tools needed to access, review and reconstruct all requested or potentially relevant electronic data.

3) Your obligations under the law are ongoing and should be considered in force and effect until the resolution of this matter. Accordingly, with regard to electronic data and documents that are created subsequent to the date of this Subpoena, relevant evidence is not to be destroyed or overwritten and you should take whatever steps are necessary to avoid destruction of potentially-relevant evidence.

WHEREFORE YOU ARE HEREBY COMMANDED TO PRODUCE:

Unless otherwise noted, the time period applicable to the following requests is January 1, 2021 through the date upon which the response to this Subpoena is due to the Office of the Attorney General. **To prevent any potential dissemination of sensitive information, please do not include any personal information in your responses and/or supporting documentation.**

When producing documents, index the documents to correspond to each document request.

1. Documents sufficient to identify each business entity (e.g., parent, affiliate, sister, subsidiary) that collectively comprises the company. In lieu of providing the actual documents, you may identify each such business entity.

2. All organizational charts sufficient to show the relationship between each business entity identified in your response to Request No. 1.

3. Documents sufficient to show your current corporate structure.

4. Documents sufficient to show your full legal name, place of incorporation, and principal office location.

5. Documents sufficient to identify your current ownership structure.

6. Documents sufficient to identify the scope of your operations in:
   a. the United States;
   b. China; and
   c. Vietnam.

7. All documents identifying any formal or informal connection, between you and TP-Link Technologies Co., Ltd. ("TP-Link Technologies").

8. All documents related to the formal separation of you from TP-Link Technologies.

9. All documents identifying TP-Link networking products and/or components sold or distributed in the United States that are or were manufactured in Vietnam.

10. All documents identifying TP-Link networking products and/or components sold or distributed in the United States that are or were manufactured in China.

11. All documents identifying any TP-Link networking products sold or distributed in the United States that are or were manufactured outside of Vietnam and China.

12. For TP-Link networking products sold or distributed in the United States, documents sufficient to identify:
    a. All manufacturers used by you;

b. All suppliers used by you;
c. All software sources used by you;
d. All hardware sources used by you; and
e. All assembly plants used by you.

13. All documents relating to the origins of all individual components used in the assembly of all TP-Link networking products sold or distributed in the United States.

14. All documents relating to TP-Link networking products currently being sold or distributed in Florida that were manufactured prior to the separation from TP-Link Technologies, whether the products are still supported by you (e.g. in the form of software updates or vulnerability patches), and the removal of those products from the stream of commerce.

15. All documents identifying the time period in which you sold or distributed TP-Link networking products in Florida, the number of units sold or distributed directly or indirectly to individuals or businesses in Florida, and the revenue received from those sales.

16. Copies of all contracts between you and Florida retailers who sell TP-Link networking products.

17. Copies of all contracts between you and Florida internet service providers who purchase, sell and/or lease TP-Link networking products.

18. Documents sufficient to identify the locations of your research and development facilities in the United States and China, including addresses and dates of operation.

19. Documents sufficient to identify where TP-Link networking products are and have been designed, manufactured, assembled, and tested.

20. All documents related your current and past product development and testing processes.

21. All documents identifying whether you currently share any software sources with TP-Link Technologies.

22. All documents, including but not limited to correspondence, complaints, subpoenas, civil investigative demands, and written testimony, that refer or relate to any investigation of your business practices by any judicial, administrative, government, congressional, or law enforcement agency relating to your relationship with TP-Link Technologies or any TP-Link networking products.

23. All documents between you and the U.S. Department of Commerce regarding the security of TP-Link networking products.

24. Documents sufficient to identify the names and locations of all departments or entities responsible for:
    a. Firmware used in TP-Link networking products,
    b. Software updates for TP-Link networking products and apps, and

c. TP-Link networking product and app development and updates.

25. All documents identifying all entities with access to the source code for firmware used in TP-Link networking products sold or distributed in the United States.

26. All documents identifying where software updates for TP-Link networking products originate, including the provider(s) and their location(s).

27. Documents sufficient to identify your cloud platform service provider(s) and the data center location(s) storing and/or otherwise processing United States consumer data.

28. All documents identifying your current and past supply chains during the relevant time period and how you maintain control over these supply chains.

29. Any documents related to the claims on the company's website at https://www.tp-link.com/us/landing/security-commitment/ that:
    a. "As a company headquartered in the United States, no government — foreign or domestic — has access to and control over the design and production of our routers and other devices."
    b. "TP-Link Systems is no longer affiliated with the China-based TP-Link Technologies, which sells exclusively in mainland China."
    c. "Our internal penetration testing team, composed of experienced professionals, skilled in IoT and embedded systems security, conducts continuous threat modeling and real-world simulation attacks."
    d. "[W]e work with accredited third-party security labs to scrutinize our products and help us identify, prioritize, and promptly address potential vulnerabilities before they affect our customers."
    e. "[P]ublic vulnerability data (sourced from recognized security repositories like CVE Details and VulDB) shows that TP-Link's rate of vulnerabilities per product is significantly lower than those of other leading manufacturers."
    f. "[W]e offer prompt firmware updates and publish detailed security advisories, ensuring that we can rapidly deliver patches and enhancements to keep users safe."
    g. "We also maintain clear end-of-life policies, ensuring devices continue to receive critical updates wherever possible."

30. Documents sufficient to identify the "accredited third-party security labs" referenced in Request No. 27(d).

31. Copies of all versions of https://www.tp-link.com/us/landing/security-commitment/ or any of your consumer-facing cybersecurity webpages during the relevant time period.

32. Copies of any of your marketing materials relating to privacy and security of TP-Link networking products.

33. Copies of all privacy policies relating to TP-Link networking products during the relevant time period.

34. All documents relating to how you are complying with your privacy policies.

35. All documents identifying all types of personal information ("PI") collected from or about consumers in the United States in connection with the use of any TP-Link networking products, the reason for the PI collection, the retention period, and location the PI is stored.

36. All documents identifying the names and locations of all departments or entities that have access to any PI collected from or about consumers in the United States and stored by you.

37. All documents relating to reports or investigations of the privacy or security of TP-Link networking products.

38. Copies of all customer complaint handling policies and procedures relating to TP-Link networking products.

39. For each TP-Link networking product, all warranties you have provided and a representative copy of each such warranty that you have provided to Florida internet service providers, retailers, consumers, and purchasers.

40. Copies of all consumer complaints you have received regarding privacy and security vulnerabilities of TP-Link networking products, and all documents relating to how you handled and resolved these consumer complaints.

41. Copies of any security and risk management policies and procedures relating to your handling of cybersecurity vulnerabilities.

42. Copies of all cybersecurity policies relating to TP-Link networking products during the relevant time period.

43. All documents relating to how you are complying with your cybersecurity policies.

44. All documents relating to how you notify consumers about cybersecurity vulnerabilities, vulnerability patches, firmware updates, and software updates.

45. All documents relating to any of your internal studies and/or investigations into hacking or vulnerabilities of TP-Link networking products.

46. All documents identifying a security vulnerability or the hacking of TP-Link networking products sold or distributed in Florida, and the steps you took to address the vulnerability or hacking.

47. All documents to support your claim of making products that follow the principles of CISA's Secure-by-Design pledge.

48. All documents between you and CISA regarding the security of TP-Link networking products.

49. Relating to Microsoft Threat Intelligence's statements at https://www.microsoft.com/en-us/security/blog/2024/10/31/chinese-threat-actor-storm-0940-uses-credentials-from-password-spray-attacks-from-a-covert-network/ :
    a. All documents between you and Microsoft related to CovertNetwork-1658.
    b. All documents relating to any of your investigations into CovertNetwork-1658.
    c. All documents relating to what steps, if any, you have taken to address CovertNetwork-1658.
    d. Any documents between you and consumers related to CovertNetwork-1658.

50. Relating to the CATO Network's statements at https://www.catonetworks.com/blog/cato-ctrl-ballista-new-iot-botnet-targeting-thousands-of-tp-link-archer-routers/:
    a. All documents related to any of your investigations into the IoT botnet Ballista.
    b. All documents relating to what steps, if any, you have taken to address Ballista.
    c. Any documents between you and consumers related to Ballista.

51. Regarding "HomeShield", all documents to support the claims made at https://www.tp-link.com/us/homeshield/ that HomeShield "handles all your concerns" on:
    a. "Private Info Leakage."
    b. "Cyber Virus Intrusion."
    c. "IoT Device Attacks."
    d. "Internet Addiction."

52. All documents to support the claims made at https://www.tp-link.com/us/homeshield/ that HomeShield "provides comprehensive security protection" with "100% safeguard" using "advanced algorithms to protect all your IoT and other connected devices from any cyber threats and attacks."

53. All documents identifying the types of PI collected from or about consumers in the United States for the HomeShield service.
    a. If PI is collected for HomeShield, all policies on security, retention, and access of the PI, and the location(s) the PI is stored.

54. All documents identifying the types of PI collected from or about consumers in the United States for the KidShield service.
    a. If PI is collected for KidShield, all policies on security, retention, and access of the PI, and the location(s) the PI is stored.