# Cisco Transparency and Law Enforcement Demands for Customer Data

Cisco is committed to publishing data regarding demands for customer data that we receive from law enforcement and national security agencies around the world. We publish this data twice yearly (covering a reporting period of either January-to-June or July-to-December). Cisco reports these numbers with a six-month delay.

The tables that follow list the number of demands Cisco has received from United States federal, state or local law enforcement during the stated time period. A table with demands from non-U.S. governments follows. Cisco also breaks out and separately reports demands by non-US governments for data that is stored either in the U.S. or in another jurisdiction (country or region) outside of the United States through CLOUD Act Executive Agreements.

NOTE: If a single demand includes both customer and non-customer data, Cisco reports these as two individual demands. Further, the numbers listed in the columns titled *No Data Disclosed* include demands for which Cisco was unable to identify responsive data as well as demands for which Cisco determined the accompanying legal process to be insufficient.

### Government Data Demands — United States

| July 1 - December 31, 2018 | Total Demands | No Data Disclosed | Data Disclosed |
|---|---|---|---|
| Customer Data | 5 | 5 | 0 |
| Non-Customer Data | 20 | 17 | 3 |
| Emergencies | 0 | 0 | 0 |

### Government Data Demands — International

| July 1 - December 31, 2018 | Total Demands | No Data Disclosed | Data Disclosed |
|---|---|---|---|
| Customer Data | 0 | 0 | 0 |
| Non-Customer Data | 21 | 0 | 21 |
| Emergencies | 0 | 0 | 0 |

### CLOUD Act Executive Agreement Demands

| July 1 - December 31, 2018 | Total Demands | No Data Disclosed | Data Disclosed |
|---|---|---|---|
| Customer Data | 0 | 0 | 0 |
| Non-Customer Data | 0 | 0 | 0 |
| Emergencies | 0 | 0 | 0 |

### Customer and Non-Customer Data

Customer Data is all data (including text, audio, video or image files) that is provided to Cisco in connection with your use of our products or services. Customer Data does not include Administrative Data, Payment Data, Support Data or Telemetry Data, as defined in the Data Definitions document. Demands that do not fall into the Customer Data category are listed as "Non-Customer Data."

### Emergency Demands

Law enforcement may demand information from Cisco that is needed to help resolve serious emergencies. Cisco is authorized by federal law to provide the requested information in such emergencies and we have an established process to respond to emergency demands, in accordance with the law.

### Cisco's Principled Approach

Cisco carefully reviews each demand we receive. Cisco's Principled Approach to Government Requests for Data outlines how Cisco protects customers while assisting law enforcement under the appropriate legal conditions. The Trust Center is the best source of information on how Cisco is Trustworthy, Transparent and Accountable to our customers.

### United States National Security Demands

Cisco may receive demands for data from U.S. national security organizations. This includes Foreign Intelligence Surveillance Act (FISA) warrants, orders, directives, or National Security Letters (NSLs). The table below lists the number of U.S. National Security demands Cisco has received during the applicable period. Cisco reports these numbers with a six-month delay. The USA Freedom Act of 2015 specifies that these demands be reported within a range of numbers.

### United States National Security Demands

| July 1 - December 31, 2018 | Totals |
|---|---|
| National security orders, directives, or national security letters received | 0-249 |
| Number of accounts affected under all national security orders, directives, or national security letters | 0-249 |