# Cisco Transparency Report: Government Demands for Data

## Reporting Period: Jan 1st – June 30th, 2022

Cisco is committed to being transparent about demands for customer data received from government and law enforcement agencies globally. We publish transparency reports twice yearly, one covering a reporting period of January to June and the other covering July to December. Each report is published six months following the end of the reporting period.

The following tables list the total number of demands for customer data received from government and law enforcement agencies by type of customer data demanded. This includes the number of demands that were rejected, the number of demands that did not result in disclosure, and the number of demands that resulted in disclosure.

# Reporting Period: Jan 1st - June 30th, 2022

### Government Data Demands – United States (exclusive of National Security Demands, which are reported below)

| Data Type Demanded | Total Demands | No Data Found | Total Rejected | Total Disclosed |
|---|---|---|---|---|
| Content Data | 1 | 0 | 1 | 0 |
| Non-Content Data | 21 | 10 | 7 | 4 |
| Emergencies | 3 | 0 | 2 | 1 |

### United States National Security Demands

Cisco may receive demands for data from U.S. national security organizations. These include 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, subject to the limitations prescribed by the USA Freedom Act of 2015.

| Demands Received Jan 1st-June 30th, 2022 | Totals[1] |
|---|---|
| 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 |

# International Demands

### Government Data Demands – Germany

| Data Type Demanded | Total Demands | No Data Found | Total Rejected | Total Disclosed |
|---|---|---|---|---|
| Content Data | 0 | 0 | 0 | 0 |
| Non-Content Data | 42 | 1 | 3 | 38 |
| Emergencies | 0 | 0 | 0 | 0 |

[1] Cisco is required to use bands when publicly reporting the below information. See 50 U.S.C. § 1874.

### Government Data Demands – Poland

| Data Type Demanded | Total Demands | No Data Found | Total Rejected | Total Disclosed |
|---|---|---|---|---|
| Content Data | 0 | 0 | 0 | 0 |
| Non-Content Data | 1 | 0 | 0 | 1 |
| Emergencies | 0 | 0 | 0 | 0 |

### Government Data Demands – India

| Data Type Demanded | Total Demands | No Data Found | Total Rejected | Total Disclosed |
|---|---|---|---|---|
| Content Data | 0 | 0 | 0 | 0 |
| Non-Content Data | 3 | 1 | 1 | 1 |
| Emergencies | 0 | 0 | 0 | 0 |

### Government Data Demands – Netherlands

| Data Type Demanded | Total Demands | No Data Found | Total Rejected | Total Disclosed |
|---|---|---|---|---|
| Content Data | 0 | 0 | 0 | 0 |
| Non-Content Data | 1 | 1 | 0 | 0 |
| Emergencies | 0 | 0 | 0 | 0 |

### Government Data Demands – United Kingdom

| Data Type Demanded | Total Demands | No Data Found | Total Rejected | Total Disclosed |
|---|---|---|---|---|
| Content Data | 0 | 0 | 0 | 0 |
| Non-Content Data | 2 | 0 | 1 | 1 |
| Emergencies | 0 | 0 | 0 | 0 |

### Percent Disclosed – US and International Demands Combined

| Jan 1st-June 30th, 2022 | Total | % Disclosed |
|---|---|---|
| Content Demands Received | 1 | 0% |
| Non-Content Demands Received | 70[2] | 64% |

### Preservation Requests

A preservation request asks that data be saved for a specified period of time in anticipation of a legal process (i.e., search warrant, court order, etc.) to ensure data is not tampered with, destroyed, or lost before the legal process can be concluded. This time frame is specified in the preservation request and may result in data being stored longer than its standard retention period.

### Preservation Requests – United States

| Jan 1st-June 30th, 2022 | Total Preservation Requests | No Data Found | Total Rejected | Total Preserved |
|---|---|---|---|---|
| Preservation Requests Received from the United States | 2 | 0 | 0 | 2 |

### Preservation Requests – International

| Jan 1st-June 30th, 2022 | Total Preservation Requests | No Data Found | Total Rejected | Total Preserved |
|---|---|---|---|---|
| Preservation Requests Received from outside of the United States | 0 | 0 | 0 | 0 |

[2] Calculation is inclusive of the three US emergency demands received, which were for non-content data.

# Frequently Asked Questions

### Q. How does Cisco respond to Government Data Demands?

Cisco assesses and responds to government and law enforcement demands for customer data in accordance with Cisco's Terms of Service, privacy policies, and applicable law. We carefully review each demand we receive to ensure we are protecting the privacy of our customers while meeting our legal obligations. For more detail on how we respond to demands for customer data, please see our Principled Approach to Government Demands for Data. The Trust Center is the best source of information on how Cisco is trustworthy, transparent, and accountable to our customers.

### Q. What is the difference between content and non-content data?

Cisco categorizes data into three categories: Systems Information, Personal Data, and Customer Content. These definitions are outlined in the Data Management page of Cisco's Trust Center, as well as in the data briefs hosted on the Cisco Trust Portal. U.S. law places a higher burden on government requests for content data than non-content data. Content data aligns to Cisco's "Customer Content" (formerly "Customer Data") classification, and includes text, audio, video, or image files our customers create in connection with the use of Cisco products or services. Non-content data generally aligns to Cisco's "Systems Information" and "Personal Data" classifications, and includes basic subscriber information such as name, address, phone number, IP address and email address, payment data such as credit card information, and telemetry data generated in connection with the customer's use such as URLs, net flow data, and information relating to the existence of cookies.

### Q. What is an emergency data demand?

Law enforcement may demand information from Cisco that is needed to help resolve imminent threats to life or serious physical harm. Where authorized by applicable law, Cisco may provide information in such emergencies, and we have an established process to respond to emergency demands.

### Q. Does Cisco ever challenge government demands for data?

Cisco challenges or rejects all data demands that are not accompanied by a valid legal process or a valid legal basis. Our legal team seeks additional clarification from government and law enforcement officials to clarify or narrow the scope of demands that are unclear or overly broad.

### Q. How has Cisco responded to the CLOUD Act?

Cisco believes that governments and law enforcement agencies should go directly to customers for content and non-content data demands in the first instance. All requests received by Cisco, whether under the CLOUD Act or not, are carefully reviewed to ensure we comply with applicable law and Our Principled Approach to Government Demands for Data.

### Q. If Cisco receives a demand for customer information, will Cisco tell the customer about it?

Cisco's policy is to notify customers before producing data in response to legally valid demands unless such notification to the customer is prohibited by applicable law, or emergency circumstances prevent advance notification. Where demands that prohibit notification to the customer are excessive in duration (over one year in length), or are overly broad in scope, Cisco will challenge the demand to protect our customer's legitimate interests. For more information, please see Our Principled Approach to Government Demands for Data.

### Q. Why do some new reports show more information than older reports?

We are constantly working to improve our internal processes and to bring increased transparency to our customers. As a result, we have expanded this report to include country-level information on demands, the number of demands Cisco rejected, the percentage of demands where data was disclosed, and the number of preservation requests we have received.

### Q. Why are only certain countries represented on this report?

Countries that provided a government data demand to Cisco during the current reporting period are represented above. If a country isn't included in the tables above, Cisco did not receive any data demands in that jurisdiction during the reporting period.

### Q. Does Cisco ever give governments direct access to content or non-content data, or create backdoors?

Cisco never gives governments or law enforcement agencies access to content or non-content data without following the appropriate legal process. Consistent with Cisco's Security Vulnerability Policy, our product development practices specifically prohibit any intentional behaviors or product features that are designed to allow unauthorized device or network access, exposure of sensitive device information, or a bypass of security features or restrictions (including, but not limited to, undisclosed device access methods or "backdoors").

### Q. How does Cisco consider Human Rights when responding to Government Data Demands?

Cisco's approach to respecting human rights is outlined in our Global Human Rights Policy, which is grounded in the United Nations Guiding Principles on Business & Human Rights. Our Principled Approach to Government Data Demands is designed to minimize disclosure of customer data, uphold and respect human rights, and promote accountability and transparency with our customers and the public.

### Q. How can government agencies send legal demands to Cisco?

If you are an official representative of a Government or Law Enforcement agency and you are seeking data from Cisco, you may submit your legal demand via Cisco's government data request intake process. If government and law enforcement agencies have served the legal process by email to the above intake form, there is no need to serve a duplicate hardcopy process on Cisco by mail.