Compromised Equipment Return-to-Service (CERTS)
Customer Information

OVERVIEW

From time to time, a contamination event (ranging in significance from a hurricane, flood, fire or act of terrorism to infiltration of humidity and construction dust) may significantly harm Cisco equipment owned or leased by customers. Equipment that has been compromised by a disaster or contamination event is not eligible for advance replacement under a Cisco warranty or service contract return materials authorization (RMA) process.

Cisco's Non-Entitlement Policy for Destroyed Products can be found here:
http://www.cisco.com/en/US/prod/prod_warranty0900aecd8013f245.pdf.

Cisco's List of Services Not Covered can be found here:
http://www.cisco.com/legal/Services_Not_Covered.pdf.

After contamination, customers frequently ask Cisco to determine if their equipment is operational and maintainable. In response, Cisco requests that customers follow the Compromised Equipment Return-to-Service (CERTS) process to determine under what circumstances (if any) the impacted Cisco equipment may be re-entitled for Cisco maintenance and/or other Cisco services. Under the CERTS process, customers engage third-party analysis firms (who use specific, Cisco-approved testing techniques and procedures) to determine the contamination status of impacted Cisco equipment. CERTS program administrators base their decision whether or not to re-entitle impacted equipment largely on these results. Analysis and any subsequent cleaning done in accordance with the CERTS process do not guarantee reinstatement of equipment to serviceability.

INITIAL CONTACT

In the event of a disaster or other contamination event that may have impacted Cisco equipment, the customer (meaning either the end-user customer purchaser or lessee of Cisco equipment, or the Cisco reseller who is supporting the end user customer) should notify its Cisco account team as soon as possible. The account team will then coordinate with Cisco's CERTS team to follow Cisco's policies, answer any questions and respond to any customer requests.

REQUIRED INFORMATION

After a customer notifies Cisco, the Cisco account team will provide the customer with a questionnaire, which asks for information about the event and the impacted equipment, such as:

- Timeline of Events – describing what occurred that would cause the equipment to become suspect.
- Inventory List of Equipment – including serial numbers, model numbers, device names, locations in building and any other relevant information.
- Floor Plan / Building Layout – including square footage, number of floors, location and quantity of closets per floor, with data centers and critical technology areas indicated.
- Occupancy Documents – issued by either the customer's local government (i.e. city/county) or an outside certification party, stating that the facility is suitable for occupancy. Proper documentation could include an air quality statement, an engineering firm's remediation statement, or similar document. These documents must be provided before any Cisco employee may visit a customer site following a disaster. (For more information, see "Safety of Cisco Employees" below.)

EQUIPMENT INSPECTIONS

Based on the customer's answers to the questionnaire, Cisco and the customer will determine if an inspection of the potentially contaminated equipment is necessary. In some cases, it may be clear that a customer's equipment was exposed to adverse environmental conditions that substantially impacted its functionality, and cannot be serviced. In other cases, more information may be needed to make an assessment of the equipment's status, and Cisco may recommend that an inspection be performed by a qualified third party inspection company.

Cisco does not inspect or test Customer equipment. Instead, in cases where the level of contamination or functionality of equipment is in question, a third party that meets Cisco's inspection and testing protocols should perform the inspection. While Cisco does not have a formal vendor certification program, Cisco will accept inspection reports only from third party companies that meet Cisco's strict testing and cleaning protocols. (For example, Cisco requires ion chromatography testing and IPC-accepted protocols for cleaning.)

Cisco recommends the following qualified, independent third party company perform the inspection:

Coastal Technical Services, http://www.coastaltechservices.com

If customers wish to engage a party other than named above, they should contact Cisco to have the proposed testing and cleaning protocols evaluated by Cisco before any engagement or inspection. (Please be cautioned that some inspection companies may incorrectly claim that they test and clean equipment using "Cisco-certified" personnel or Cisco-authorized procedures.)

If an inspection is necessary (by either the specific testing company named above, or by another company that meets Cisco's strict testing and cleaning protocols), customers should make arrangements directly with the inspection company for all services, without involvement by Cisco. The contract for inspection and all payment terms should be discussed directly between the customer (and/or its insurance company) and the third party inspection company. Similarly, if any questions or issues arise regarding insurance claims or procedures, customers should contact their insurance companies directly, without involvement by Cisco. All insurance procedures and payments are between the customer and its insurance company.

SAFETY OF CISCO EMPLOYEES

Safety is of utmost importance at Cisco, and is typically a significant concern following a disaster. Customers should understand that Cisco personnel are prohibited from visiting any work or other hazardous sites unless certain internal clearances are granted at a vice president level. It is Cisco's policy that before any Cisco employee may visit a customer site affected by a disaster, Cisco must first obtain from the customer a current Certificate of Occupancy (COO), as issued by the appropriate city or county government. If no COO is available, Customers must provide copies of written reports by certified environmental consultants and structural engineers that confirm the premises at issue are acceptable for re-occupancy, in accordance with federal, state and local laws and regulations.

For further information, please contact your Cisco account team representative, who will work with Cisco's CERTS Team to respond as promptly as possible to all customer requests.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**