A customer guide to cloud.gov

A guide to how to contact us, the division of responsibilities between cloud.gov and you, and what happens if something goes wrong.

This is a supplement to our formal documents: our Inter-Agency Agreement with each customer and our FedRAMP JAB P-ATO documentation. The System Security Plan in the P-ATO documentation provides formal details about platform customer responsibilities, and you can request a copy.

Overall division of responsibilities

cloud.gov is responsible for the cloud.gov platform, including maintenance, security, and compliance. We are responsible for ensuring a FISMA Moderate level of confidentiality, integrity, and availability for the platform.

Customers are responsible for their own resources on cloud.gov, including managing permissions and access, as well as operating and securing their applications.

Contact methods and response times

Our primary support method is email: cloud-gov-support@gsa.gov. We aim to respond within 1 business day for emails. We answer incoming mail between about 9 am - 8 pm Eastern time.

To contact us outside of business hours when necessary, we also have an emergency email address: cloud-gov-emergency@gsa.gov. This inbox enables emails from whitelisted email addresses to alert us off-hours. Customers should tell us (via email to cloud-gov-support@gsa.gov) a list of email addresses to whitelist for access to the emergency email. Currently, we make a best-effort to watch for these alerts outside business hours, although we cannot yet guarantee an off-business-hours response.

Handling security incidents

Report a security problem in the cloud.gov platform

If you notice a potential security incident or security vulnerability in the platform itself, use our contact methods (above). We follow a formal security incident response procedure, coordinated with GSA IT, which includes appropriate steps for notifying any affected customers.

Request help from cloud.gov with a security problem in your application

If you have a security incident in your system and you need assistance of some kind from the cloud.gov team, such as recovering permissions, use our contact methods.

How we report security problems that affect you

If we identify a security incident or vulnerability that affects your account or applications on cloud.gov, we will email the System Owner as soon as possible, and work with them on follow-up steps. If we have no designated System Owner on record, or if that email address bounces, by default we contact the Org Managers.

To prevent false positives: inform us of penetration tests or major load tests

If you plan a penetration test of your applications, you should notify us ahead of time by emailing our support mail.

If you plan a major load/stress test of your applications, it’s helpful to send a quick note to our support mail ahead of time, so that we understand any unusual results in our platform monitoring.

Incident response details

Additional details are in the cloud.gov System Security Plan IR (Incident Response) controls.

Maintenance of security posture

As a product with a FedRAMP Joint Authorization Board P-ATO, we are required to go through the FedRAMP JAB Significant Change Request review process before making major changes to the architecture of the platform.

We send monthly continuous monitoring reports to the JAB, and we go through an annual FedRAMP re-assessment with a third-party assessment organization (3PAO) and the JAB.

Platform availability and performance

We provide public notice of service disruptions at https://cloudgov.statuspage.io/ — including updates on resolution progress during a disruption.

We also give notice there for occasional scheduled maintenance windows for developer tools, where developer-facing features (such the command line tools or log viewer) may be unavailable.

We encourage customers to use the page's option to subscribe to notifications.

If a customer application has a problem, the customer team is responsible for diagnosing whether the problem is caused by the platform or the application. If you're not sure after checking, contact us. We can assist with diagnosing whether the cause is in the platform.

Additional details are in the cloud.gov System Security Plan CP (Contingency Planning) controls.

Escalations

First contact the cloud.gov team using the contact methods. These methods reach our team directly, including our operations engineers and leadership.

The acting director of cloud.gov is Shashank Khandelwal (shashank.khandelwal@gsa.gov), and the acting deputy director of cloud.gov is Britta Gustafson (britta.gustafson@gsa.gov).

cloud.gov is part of the Technology Transformation Services in the General Services Administration.