



## Offering Description:

# CGI Federal Cloud Infrastructure as a Service (IaaS)

U.S. General Services  
Administration Blanket  
Purchase Agreement (BPA)

CGI Schedule Contract  
Number: GS-35F-4797H

CGI BPA Number:  
GS00Q11AEA0005

Award Date: 10/15/2010  
Expire Date: 10/14/2015  
Period of Performance: 5 years

## Contents

<b>Introduction</b>	1
<b>CGI Federal Cloud IaaS Overview</b>	2
Service, Not Just Servers	3
Using the BPA	3
BPA Lots	3
Lot 2: Virtual Machines (VMs)	4
Lot 3: Cloud Web Hosting Services	5
<b>Features of CGI's Federal Cloud IaaS</b>	9
On-demand provisioning for power and control	9
Automated service management for alignment and accountability	11
New Customer Activation	12
Help Desk	12
Scheduled Maintenance	12
Incident and Problem Management	12
Service Level Agreements (SLAs)	13
Security for protecting the majority of government's IT workload	14
Authority to Operate	14
Secure Data Center Environments	14
Access Control and Credentials Management	15
Encryption of Data—Rest/Transit	15
Managed Security Services	16
CGI and Customer Security Responsibilities	16
Information services for predictable and sustainable savings	17
Billing	17
Threshold Notification	18
Performance and Utilization Monitoring	18
Trending and Reporting Capabilities	19
Event Tracking and Audit Controls	20
Additional Services Available Under GSA IT Schedule 70	20
Transition and Migration Services	20
Proof of Concept/Roadmap	21
Security Advisory Services	21
<b>For more information</b>	21

## Introduction

Cloud computing enables the agile and innovative use of information technology at a fraction of the cost of traditional IT infrastructure. It provides cost-effective solutions for agencies that require application and Web hosting and/or have episodic needs such as development and test, fast-growing or shrinking demand, predictable and unpredictable peaks and mandated new or upgraded applications.

As a full-service cloud provider, CGI combines certifications, infrastructure and IT service management for all aspects of the cloud. Our cloud services are backed by 35 years of IT infrastructure and managed services experience for government and commercial organizations. Cloud is an integral part of our \$1 billion infrastructure business which serves more than 180 CIOs and over 50 U.S. federal agencies or programs. We provide the expertise, processes and governance to help organizations navigate the transition, integration and ongoing management of the cloud.

CGI was competitively awarded the U.S. General Services Administration's Blanket Purchase Agreement (BPA) for Infrastructure as a Service (IaaS) on October 15, 2010. The BPA enables agencies to obtain cloud IaaS using a single, fixed-price Task Order. As a BPA holder, CGI is required to provide detailed pricing for explicitly defined, standard services, as well as to meet a rigorous set of technical and security requirements. CGI has met and in many areas exceeded these requirements.

In August 2011, CGI was granted Authority to Operate (ATO) on the BPA. The ATO's Assessment & Accreditation process ensures that CGI meets all of the BPA security requirements, enabling users to trust that their data is safe and secure in CGI's cloud. CGI's Federal Cloud is FISMA (Federal Information Security Management Act) compliant for Low and Moderate Impact applications—representing 88% of the U.S. government's IT workload. This includes systems that process sensitive data such as personally identifiable information (PII), Confidential Business Information (CBI) and personal health information.

The ATO also provides for continuous monitoring and reporting and an annual audit of CGI's General Support System (GSS) controls associated with National Institute of Standards and Technology (NIST) 800-53 v3 for Moderate Impact baseline. Our system security plan and associated ATO demonstrate that our controls have been validated.

BPA holders also are required to meet the essential characteristics of cloud computing defined by NIST as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

By using the BPA, agencies can be assured that their cloud provider is federally certified as secure and has an ATO.

## CGI Federal Cloud IaaS Overview

CGI's Federal Cloud IaaS can be used in Private Cloud, Community Cloud and Hybrid Cloud deployment models. It meets the NIST definition of cloud computing by providing:

- *On-demand self-service* through CGI's automated Federal Cloud Portal
- *Broad network access* to the Portal via the Internet
- *Resource pooling* where users generally have no control or knowledge over the exact location of provided resources, but can specify location for Disaster Recovery/Continuity of Operations (DR/COOP) purposes
- *Rapid elasticity* where resources can be provisioned and de-provisioned within moments
- *Measured service* and resource usage that is monitored, controlled and reported, providing transparency for both CGI and the customer.

CGI's Federal Cloud IaaS complies with the BPA's technical requirements by providing:

- An automated system that adheres to ITIL-based IT Service Management
- FISMA Moderate Impact security as defined in NIST's Federal Information Processing Standard (FIPS) Publication 199
- 99.5% availability as standard, with higher availability as an optional service
- 1 Gigabit Internet access, with dedicated access available as an optional service
- Two (2) Tier III data centers in the continental United States, separated by multiple time zones
- A cloud available exclusively to U.S. federal, state, local and tribal entities and operated in the U.S. by personnel who have passed U.S. government background investigations
- Ability to track charges with a summary invoice, detailed breakdowns (providing the number, names and types of Virtual Machines and Contract Line Item Numbers, as well as data transferred I/O and additional storage purchased information), as well as a statement of the previous bill and the current bill, updated weekly

Additional performance features include:

- CPUs—most with a speed of 1.86 GHz
- Bandwidth between VMs with:
  - Throughput for data storage of 10Gbps
  - SAN throughput of two (2) 8 Gbps SAN links
  - No minimum bandwidth with maximum constrained at 10 Gbps
  - Peering to Tier I Internet Service Providers
  - Robust LAN to meet demanding requirements

## Service, Not Just Servers

CGI's Federal Cloud IaaS also includes numerous other enterprise-class features. Moving to the cloud takes a combination of technology management, automated service management and solid transition planning to extract and maintain the value of the cloud infrastructure services.

CGI is a full-service IT firm offering service, not just servers, to realize the full benefits that drew agencies to the cloud in the first place. Automated service management is built into our standard offering, along with a host of additional services that agencies have indicated they will need in order to take full advantage of cloud technologies and services.

While the BPA provides general guidelines, CGI's Federal Cloud IaaS can easily be customized to meet unique customer needs. We work closely with customers to determine their specific requirements and to devise effective solutions using the BPA elements.

## Using the BPA

The BPA may be used by any entity within the federal government, and by state, local and tribal governments and other entities as listed in GSA Order ADM 4800.2G, "Eligibility to Use GSA Sources of Supply and Services." Additional information, including the "GSA Blanket Purchasing Agreements Ordering Guide 2011," is available at: <http://www.info.apps.gov/node/22>

The BPA uses Contract Line Item Numbers (CLINs) to give agencies a menu approach to acquiring cloud services. Purchases can be made "by the item" based on agency or program needs. The only limits are a program's own budget and policy considerations, not technical restraints. CGI's Federal Cloud IaaS follows customer-specified "not-to-exceed" limits such as monthly dollar limits. Agencies can also purchase other services in conjunction with the BPA services using GSA IT Schedule 70.

## BPA Lots

GSA awarded BPAs in three (3) unique lots. CGI offers Lot 2 (Virtual Machines) and Lot 3 (Cloud Web Hosting). We are one of 11 awardees for Lot 2 and one of 5 awardees for Lot 3. Users can procure and provision services online through CGI's Federal Cloud Portal (Portal).

- **Lot 2: Virtual Machines (VMs)**—These on-demand virtual servers are fully controlled by the government customer and are paid by the hour. Users only pay for VMs for as long as they are provisioned. There are no up-front costs and no termination charges. VMs are commonly used for development and test environments.
- **Lot 3: Cloud Web Hosting**—These Web application hosting services enable scalable, redundant, dynamic Web and application hosting and are paid by the month. CGI provides monitoring, backup and patching. Cloud Web hosting is commonly used for production environments.

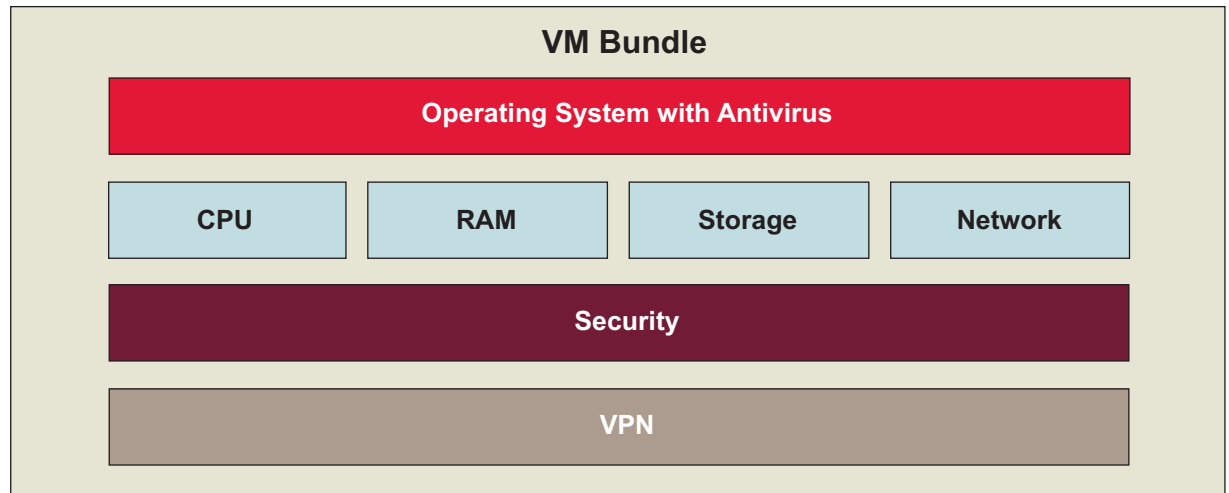
*NOTE: While CGI does not offer Lot 1 (Cloud Storage) as a stand-alone service, storage is included as part of CGI's VM and Web Hosting offerings.*

## Lot 2: Virtual Machines (VMs)

### Overview

CGI offers a choice of five (5) VM bundles (see Table 1), all of which include: CPU, RAM, operating system (OS), user disk storage and data transferred I/O (data I/O). VM services are charged by the hour (except for data I/O). Service highlights include:

- Robust fault tolerant infrastructure—99.5% availability
- Documented Service Level Agreements (SLAs)
- Service provisioning and de-provisioning in near real time
- Managed technological refresh cycles
- Help Desk and technical support
- Support for APIs



### Capacity

CGI's VMs include a minimum CPU speed of 1.1 GHz. While the CLIN categories are provided below, clients can select the speed, RAM and disk space that best suit their requirements.

**TABLE 1: VM Bundles**

Bundle	# CPU	CPU Speed (GHz)	RAM (GB)	Disk (GB)
1GB	1	1.1	1	40
2GB	1	1.86	2	80
4GB	2	1.86	4	160
8GB	4	1.86	8	320
15.5GB	6	1.86	15.5	620

## Operating Systems

CGI's standard VM offering provides and supports the following Operating Systems (OS):

- Microsoft Windows Server 2008 R2 Data Center Edition (64-bit)
- Microsoft Windows Server 2003 Data Center Edition (32 and 64-bit)
- Red Hat Linux Enterprise Edition 5.6, 64-bit

Customers may also provide their own OS, or CGI can quote alternatives to the standard under GSA IT Schedule 70.

## OS Patching

Clients are responsible for patching the systems that are part of their VM bundles unless additional services are contracted with CGI.

## Security

CGI's basic VM bundle includes connections to the Active Directory as well as McAfee™ antivirus software installed on Windows servers. It does not include security vulnerability scanning. Customers are responsible for additional antivirus and security services. These can be purchased from CGI under GSA IT Schedule 70.

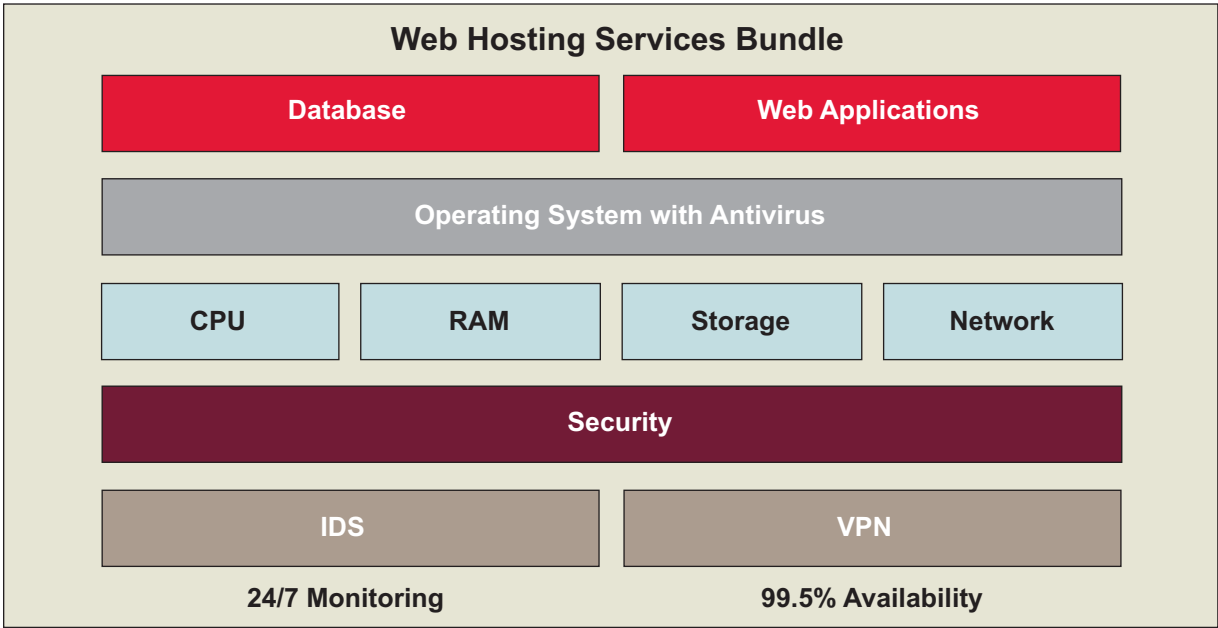
## Lot 3: Cloud Web Hosting Services

### Overview

CGI offers three (3) Web Hosting service bundles (Table 2). All bundles include CPU, RAM, OS, user disk storage, data I/O, backup and content delivery network services. Customers may also purchase Web applications and databases using the BPA.

CGI's Web Hosting services are charged by the month (except for data I/O) and include:

- Robust fault tolerant infrastructure—99.5% availability
- Documented SLAs
  - 99.5% availability, 24/7
  - Any outage of over an hour—Root Cause Analysis (RCA)
- Service provisioning and de-provisioning in near real time
- Managed technological refresh cycles
- Help Desk and technical support
- Support for APIs
- Backup and recovery
- Static IP addressing
- Vulnerability scanning, monitoring and patch management, providing embedded security to close the most common exploits
- Optional add-on for DR and COOP under GSA IT Schedule 70



Capacity

Web Hosting Service bundles include CPU speed of 1.86 GHz. Users can select either 32- or 64-bit operating systems, creating 32- or 64-bit VMs.

TABLE 2: Web Hosting Bundles

Bundle	# CPU	CPU Speed (GHz)	RAM (GB)	Disk (GB)	OS Partition (GB of Disk)	Backup (GB)	Data I/O
10GB	1	1.86	2	10	35	72	300
50GB	2	1.86	4	50	35	136	500
150GB	4	1.86	8	150	35	296	1500

Operating Systems

CGI’s Web Hosting Service bundle provides and supports the following OS:

- Windows 2003 Server Data Center Edition, 32-bit
- Windows 2003 Server Data Center Edition, 64-bit
- Windows 2008 R2 Server Data Center Edition, 64-bit
- Red Hat Enterprise Linux 5.6 64-bit with base Red Hat packages



The following web application and database options are available to customers based on the OS selected:

CLIN Type	Content of Bundle
<b>Microsoft Windows OS</b>	
• Optional Web Application (IIS)	Windows IIS Web Server Software—provides the default IIS bundle on OS chosen with .NET packages installed
• Optional Database (MS SQL Server 2008)	Microsoft SQL Server 2008 Enterprise Edition 64-bit
<b>Linux OS</b>	
• Optional Web Application (WebLogic)	Red Hat Enterprise Linux version 5 64-bit with WebLogic Server
• Optional Web Application (WebSphere)	Red Hat Enterprise Linux version 5 64-bit with the WebSphere Application Server
• Optional Web Application (Apache + PHP stack)	Apache + PHP stack
• Optional Web Application (Apache + Tomcat stack)	JBoss (includes Tomcat, Apache)—JBoss Enterprise Middleware Subscriptions Platforms and Standards Support: JBoss Enterprise Web Server 1.0.x Component versions included: <ul style="list-style-type: none"> <li>• Apache Tomcat 5.5</li> <li>• Apache Tomcat 6.0</li> <li>• Apache Tomcat Native 1.1</li> <li>• Apache Web Server 2.2</li> <li>• mod_jk 1.2.27</li> </ul>
• Optional Database (MySQL)	MySQL with Basic Level of vendor support
• Optional Database (Oracle 11g)	Oracle 11g Standard Edition 64-bit with vendor support

## Backup and Recovery

Web Hosting Service environments (data and software) include automated nightly backups to tape each business day, and storage of those tapes both onsite and at a NARA-compliant offsite facility. These backup tapes enable recovery of Web Hosting environments. Web Hosting Services customers may leverage the backups for separate application disaster recovery plans that meet their specific requirements.

- *Frequency of backups*—CGI performs backups during a scheduled, nightly backup window after each business day.
- *Frequency of restores*—Restores from backup are performed to return a system to the state it was in at the time of a scheduled backup. Restores are performed upon customer request. Customers may request one restore per VM per month.
- *Retention of backup material*—CGI retains ten (10) business days of backup.
- *Time required for retrieval and restoration of backups*—Restoration requests from customers are initiated from an onsite copy of the backup within one (1) hour of receipt from an authorized requestor. Time to complete the restoration is dependent upon the volume of data to be restored and the operating system.

## Software bundles

For databases, CGI provides the license to use the database and vendor support. The software will be installed on the Web Hosting bundle VM, ready for the customer to create and administer the databases. During backup periods, it is the customer's responsibility to ensure the database is in the proper mode for backup. For other Web Hosting software, we provide the software license with vendor support. The software will be installed ready for the customer to acquire and install Web applications, SSL certificates and other components necessary to construct a functioning system.

## OS Patching

CGI provides a hardened version of the OS (Windows Server Data Center Edition or Red Hat Linux) including vendor support. CGI performs patching for Lot 3: Web Hosting only (not for Lot 2: Virtual Machines). CGI will create a service request notifying the customer that patching is needed and requesting approval from the Contracting Officer's Technical Representative (COTR) and a security group. CGI patches on two different Saturday evenings/Sunday mornings each month, based on customer requirements. Exceptions can be made in emergency situations. OS patches are applied using BMC BladeLogic for server automation. Applications are patched either manually or using JBoss Operations Network (JON).

## Database Patching

For databases, CGI provides quarterly patching of the database software. Patching requires data to be migrated to the new patch level by the customer. To patch, CGI needs access to the user ID running the database to shut down dependent applications before the patching process starts. The customer is then responsible for starting up the database and performing any necessary data migrations once the patch operation is complete. For other Web Hosting software, we provide quarterly patching. The customer should export and save any configurations prior to the patching in the event the patching installs new configuration files.

## Security

CGI performs vulnerability scanning of the database software that we supply, and of software from other providers. Performing these scans requires a database account with select access to all schemas and objects in the database. We provide scanning results for customer review in the Portal Managed Security Services Tab.

- *OS system administration*—This comprises hardened and patched OS images in the cloud library to be used to provision a VM. We provide patches as change requests to the customer. If the customer approves the application of the patch, we will apply the patch during the maintenance window selected by the customer. Customers have administrative access to the OS. Response to the VM and OS-level incidents is the customer's responsibility unless incidents are caused by CGI's cloud infrastructure or actions.
- *Antivirus software with automatic updates of virus definitions*—For Windows-based OS, this software also provides limited blocking of inbound and outbound e-mail by preventing unregistered applications from sending and receiving e-mail. Applications that require e-mail access can be registered with our antivirus server by submitting a change request ticket.
- *System information and event management (SIEM)*—CGI performs signature-based periodic monitoring of system logs on the OS for malicious activity or errors. Logs are maintained for up to one year.
- *Security incident response*—CGI provides security incident response to alerts from antivirus, SIEM reviews, vulnerability scans and other security incident reporting. Our response is described in our security incident response plan which is available on the Portal Managed Security Services Tab. CGI requests that customers provide a point of contact and escalation plan so that we can keep customer contacts informed during an incident response. CGI reserves the right to take a Web Hosting bundle offline during a security incident response.
- *Advanced OS monitoring*—CGI monitors the health and availability of the OS with alerts sent to the customer when issues or incidents are found. This service includes dashboards of the environment showing a management view of the use and performance of the customer's services.

- *Quarterly OS vulnerability scanning*—CGI performs quarterly vulnerability scanning of the OS. We provide scan results to the customer representative who is responsible for responding to the scan results and providing CGI with a response to each item for the quarterly Plan of Action and Milestones (POAM) submission.
- *VPN Account with dual-factor authentication*—CGI supplies one dual-factor authenticated host-to-gateway VPN account with each Web Hosting machine CLIN for connectivity to the Portal and to the customer's provisioned services in the cloud.

## Additional storage

Customers may request additional storage services and will be charged by GB/hour or GB/month, depending on which package they select.

## Data transfer

Data transfer fees will be calculated by GB/month.

## Features of CGI's Federal Cloud IaaS

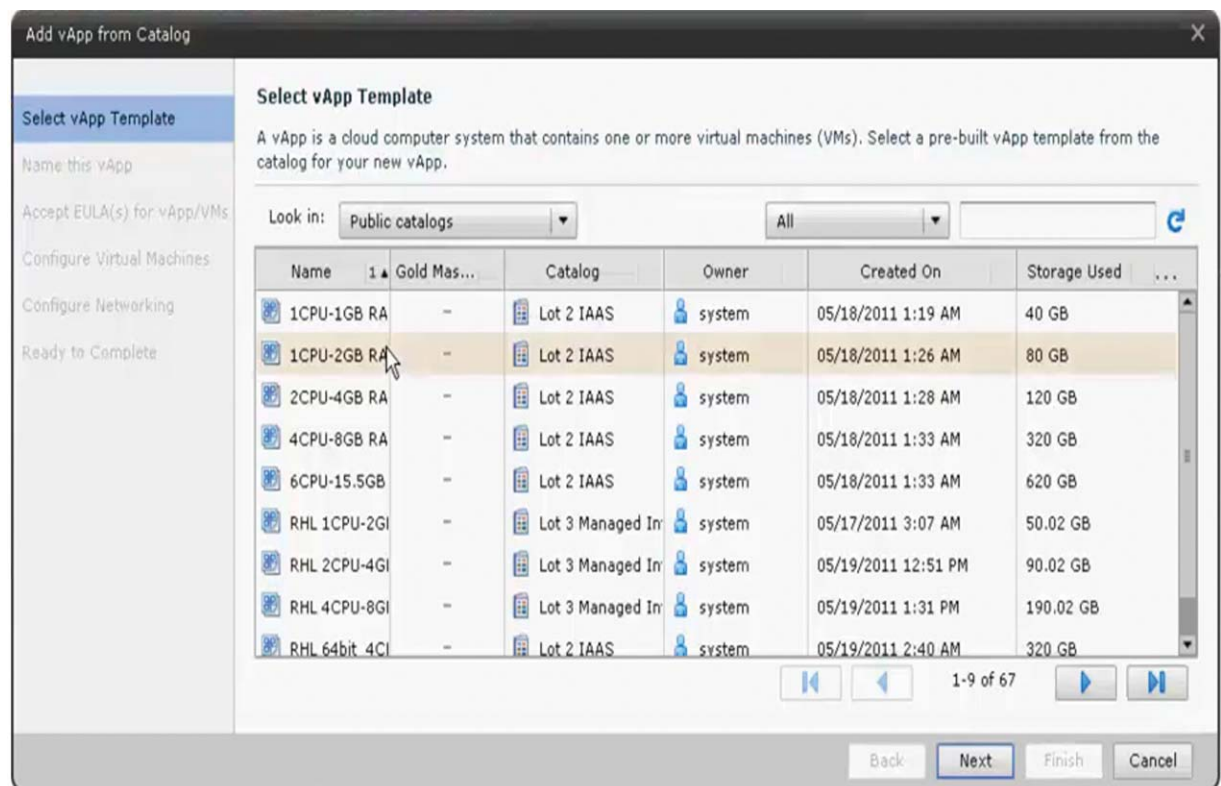
### On-demand provisioning for power and control

CGI's secure Federal Cloud Portal (Portal) enables authorized agency users to quickly and easily marshal cloud computing resources such as server time and network storage. The Portal gives users the power to design, provision and scale their environments on demand, as needed and automatically, without vendor interaction or approval delays. The Portal also provides real-time visibility and insight into service performance and cost.



The Portal uses dual-factor user authentication and a Hypertext Transfer Protocol Secure (HTTPS) connection using SSL (Secure Socket Layer) to provide secure data transmissions. A number of integrated components automate the provisioning, de-provisioning and administration of CGI's cloud services:

- Users enter new service requests through the Portal Virtual Machines Tab which includes our Service Catalog. Requests are passed to the provisioning system which orchestrates the automated provisioning of the requested items. (Note: Customers may schedule provisioning and de-provisioning events during off-hours when services can be taken offline.)
- The orchestration engine maps the business request (e.g., "create one virtual Linux server") to the multiple, underlying technical actions (e.g., "create a server, assign CPU resources, assign memory resources, allocate storage resources, load a pre-configured instance of Linux, etc.").
- The orchestration engine initiates and controls the provisioning elements, including server management, storage management and network management. These systems dynamically assign resources from a shared pool of existing resources using automated workflows and templates.
- The network management system dynamically establishes service networking components (e.g., VLANs and firewall policies), enabling customers to leverage our existing network bandwidth as well as LAN infrastructure, including the network zones, firewalls, load balancers, core switching and IP address assignment.
- Completed requests become change request records in the change management system which creates tasks that build the requested services.
- Once provisioned, a new cloud service appears on the user's view of the Portal, along with the other cloud services that user has provisioned. Provisioned services are recorded in the Configuration Management Database (CMDB).



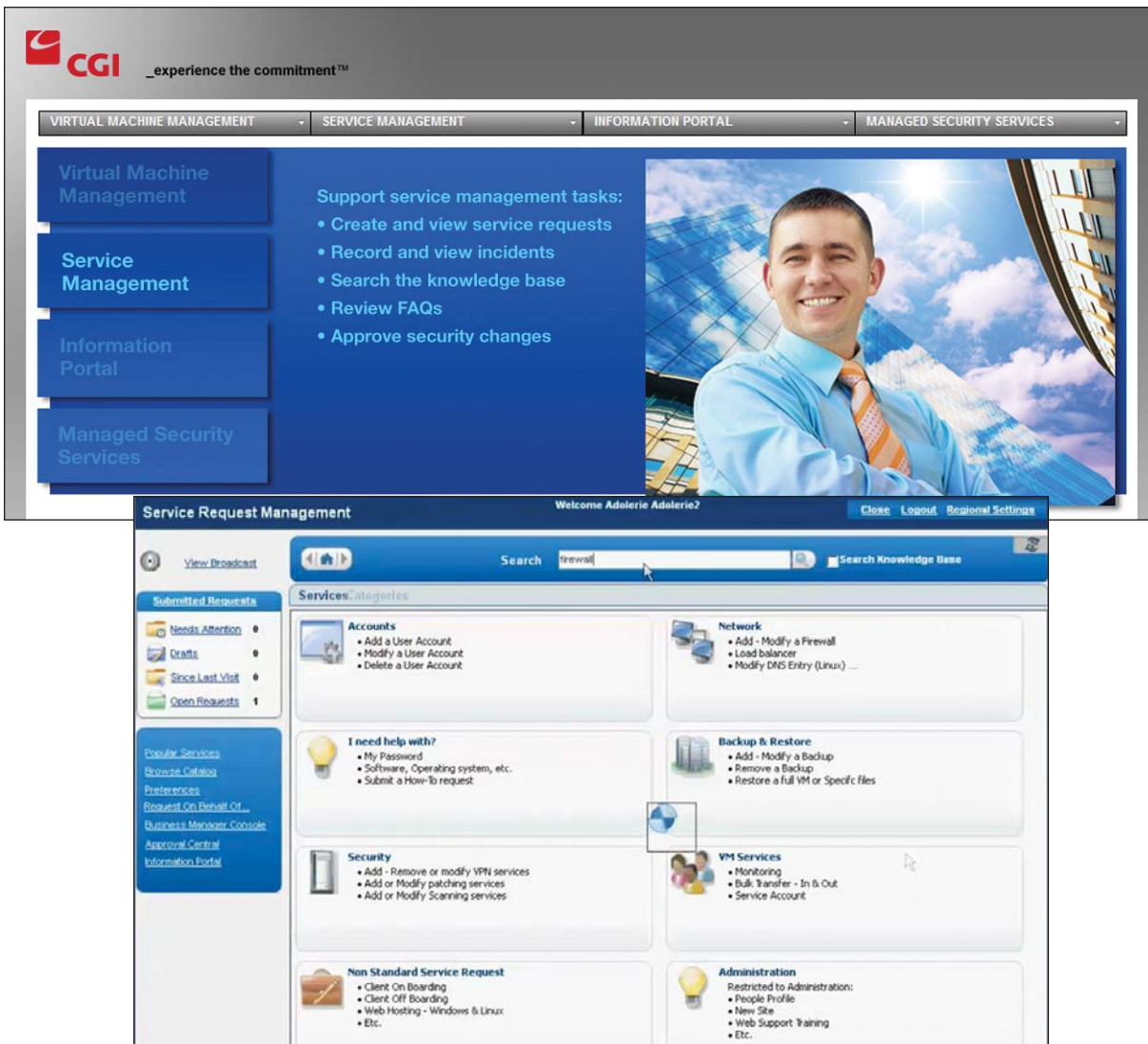


- Customers may terminate services in part or in entirety at any time. Terminations are processed through change management using the orchestration system to initiate the automated workflows. Services subscribed by a customer also contain termination dates that default to Task Order end dates or other dates set by the customer. Once a service reaches the termination date, the system creates an automated change request to initiate de-provisioning. Termination dates and times are set for each service within the CMDB, notifying the service costing system of terminations and when to stop charges. Charges for services that are paid by the hour or month will continue to the end of the charge period (hour or month).
- The same toolset provisions, administers and de-provisions services, with the CMDB providing the information about an existing service to administer or de-provision.
- If a customer wishes to close an account, the user submits a ticket or notice of termination for the Task Order to CGI. We will complete the service de-provisioning requests and then terminate the Portal account.

CGI's Federal Cloud IaaS also provides APIs that allow external systems to perform the same service provisioning request functions that are performed via the Portal.

## Automated service management for alignment and accountability

The primary objective of service management is to ensure that IT services are aligned to, and actively support, the organization's needs. When IT processes and services are implemented, managed and supported appropriately, agencies will experience less disruption, reduce costs and better achieve mission objectives.



CGI manages our network, storage, servers and virtualization using an integrated suite of service management tools designed to implement ITIL standards and processes. The tools enforce compliance with the processes, and automate operations for high efficiency, reliability, security and availability. As an example, we use several tools to perform automated continuous monitoring.

The tools are integrated with our incident management system so that monitoring alarms are automatically recorded as trouble tickets and referred to engineers for action. Our change management system controls the actions to resolve an incident, tracks change requests associated with the incident and deploys the changes. Our network management, server management and storage management systems are integrated using an orchestration engine that automates the administration and patching workflows for the network, storage, server and hypervisor layer.

### **New Customer Activation**

For a new customer, CGI establishes a customer account that includes information such as contractual terms (Task Order) and a not-to-exceed amount. We then set up billing, a VPN ID and an administrator ID for the Portal. We send the VPN and Portal login information to the customer contact. At this point, the Customer's Administrator can use the Portal to establish user IDs for other users, browse the knowledgebase, and order and provision services without further CGI intervention.

### **Help Desk**

CGI provides technical support through our Help Desk in San Antonio, Texas, on business days from 9:00 am until 5:00 pm ET. We support contact via phone, e-mail and Web chat. Phone contacts are handled through our Automatic Call Distribution (ACD), Interactive Voice Response (IVR) and Computer Telephony Integration (CTI) infrastructure. These tools increase Help Desk efficiency and caller satisfaction. Our ticketing system logs contacts and tracks them to resolution per our incident management process. The ticketing system and ACD provide the basis for extensive reporting that we use to monitor Help Desk performance and for continuous service improvement.

Support is also available on the Portal Service Management Tab, including documentation for self-help and broadcast notifications about the system such as planned maintenance and outages.

### **Scheduled Maintenance**

CGI configures our cloud service to perform maintenance while service remains available to customers. For those instances where we require a cloud-wide service interruption to perform maintenance, we schedule this well in advance of the maintenance activity and provide ample notification to customers. Our standard window for such maintenance is 9:00 pm Saturday to 9:00 am Sunday.

### **Incident and Problem Management**

Users and CGI staff use a single incident management system. The system is integrated into the Portal Service Management Tab to provide trouble ticketing functionality to users. Tickets and requests associated with the customer are viewable on the Portal, regardless of whether they are opened by the Help Desk, directly by the customer or by other sources. The user can update open tickets to provide additional information.

The Portal allows users to enter trouble tickets directly as an alternative to contacting the Help Desk. The incident management system generates management reports such as the monthly Help Desk/Trouble Tickets Report.

CGI manages and coordinates major incidents in six main phases:

<b>1. Detection</b>	Incidents are detected from the automated system or calls to Help Desk.
<b>2. Recording</b>	Incidents are recorded into the IT service management system.
<b>3. Classification and initial support</b>	Incident priority classification (1, 2, 3 and 4) depends on impact and urgency. The classification can also include a specific identification of the customer's business-critical applications that allows CGI support levels to react accordingly. Based on the classification performed, the Major Incident Management procedure can be triggered.
<b>4. Investigation and diagnosis</b>	Incidents are diagnosed based on user details, Help Desk expertise and knowledge, and pre-defined procedures and instructions.
<b>5. Resolution and recovery</b>	Resolution and recovery can be performed in most cases by Level 1 support. Level 2 and 3 support occurs upon functional escalation from Level 1. During this phase, Level 2 and 3 support has responsibility to restore/recover the incident and complete the record, but not to close it.
<b>6. Closure and review</b>	Incidents are owned by the Help Desk from beginning to end and closed only by the Help Desk upon user confirmation of the resolution. Requests for user confirmation are automatically triggered by the completion of the incident and consist of two (2) notifications: one (1) initial notice and one (1) reminder notice after 48 hours to the user who reported the incident. The user can accept or reject the resolution through the e-mail notification that is sent. Incidents are reviewed for improvement purposes and to identify the potential need for Root Cause Analysis (RCA) activities. Follow-up and SLA monitoring are performed during the entire lifecycle of the incident by the Help Desk.

Through our trouble ticketing API, we can send information on alerts triggered by our monitoring solution or security incidents. These incidents can also be updated through this API.

## Service Level Agreements (SLAs)

CGI's standard SLAs for Federal Cloud IaaS include:

- 99.5% availability
- Tracking of outage times, impacts and resolution actions
- Root Cause Analysis (RCA)
- Incident management records coupled with data captured by various monitoring tools
- Service provisioning and de-provisioning times.

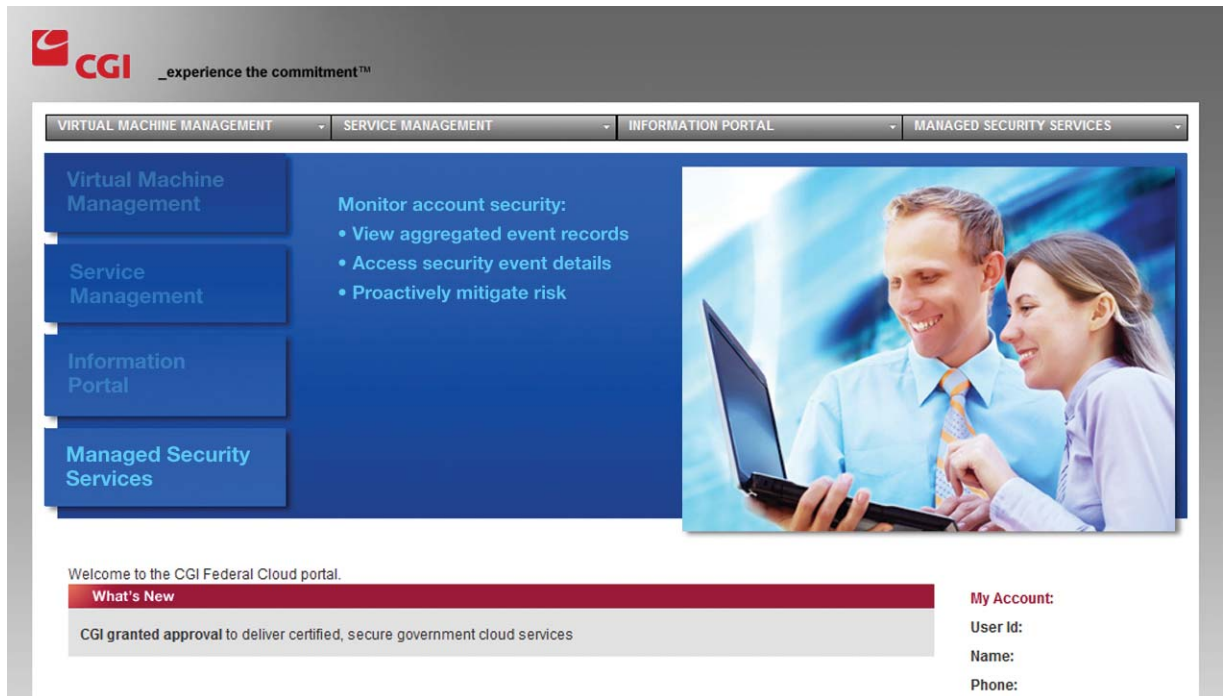
CGI is also open to more stringent SLAs per each Task Order based on mutually agreed terms.

## Penalties for not meeting SLAs

Currently under the BPA, SLAs are not associated with any specific financial penalties or incentives. Each agency's mission and use of the cloud will require different SLA's for different performance metrics. CGI provides managed services for many federal agencies and is fully comfortable with the penalty and recovery methods associated with SLAs that reflect industry standards for availability and responsiveness.

## Security for protecting the majority of government's IT workload

CGI Federal Cloud IaaS is FISMA (Federal Information Security Management Act) compliant for Low and Moderate Impact applications—which represent 88% of the U.S. government's IT workload. This includes systems that process sensitive data such as personally identifiable information (PII), Confidential Business Information (CBI) and personal health information.



14

### Authority to Operate

CGI has been awarded Authority to Operate (ATO) on the BPA, which means an audit of our General Support System (GSS) controls associated with NIST 800-53 v3 has been completed. It also ensures continuous monitoring, reporting and an annual audit. CGI's system security plan and associated ATO demonstrate that our controls have been validated.

### Secure Data Center Environments

CGI's Federal Cloud IaaS hosts all data in an enterprise Storage Area Network (SAN) that is dedicated solely to CGI's U.S. federal government customers and is located within the continental U.S. The environment is managed by individuals who have cleared HSPD-12 background investigations. Additional security features include:

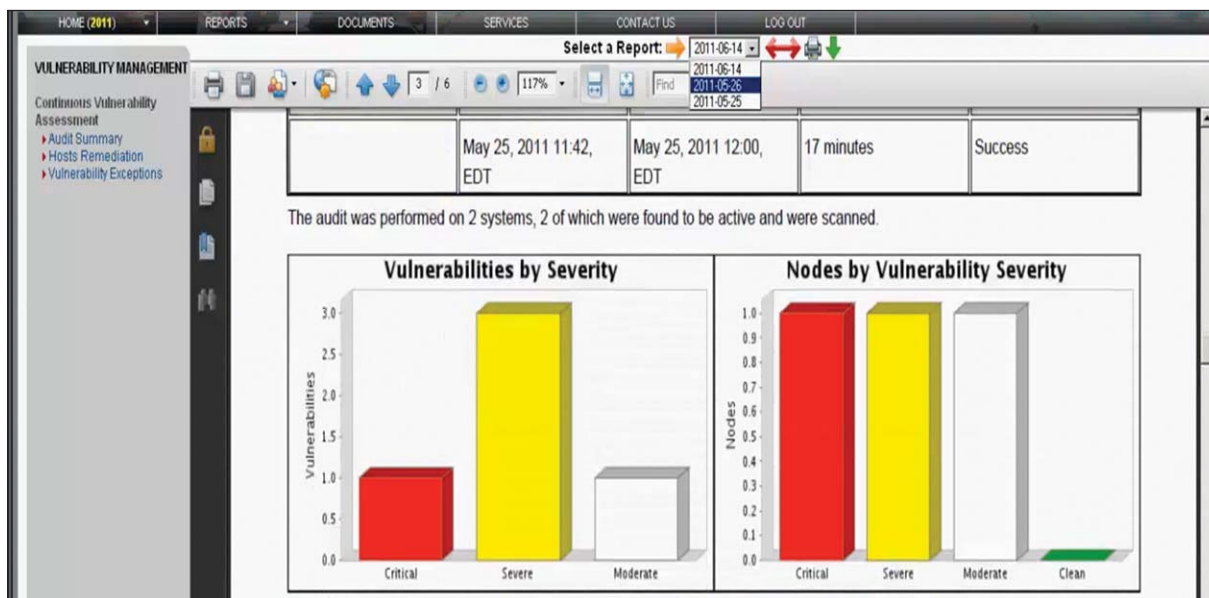
- Management of data isolation for a multi-tenant environment
- Secure service provisioning through SSL, TLS or SSH
- Secure, dual-factor remote access
- Management of data remanence through data life cycle
- Firewalls managed remotely by customers or administered by CGI at customer direction
- VMs hardened to Center for Internet Security (CIS) standards
- Security for data at rest and in transit



## Access Control and Credentials Management

CGI's Federal Cloud IaaS also includes numerous access control and identity management features, such as:

- **Access control**—Administrative access is granted through named accounts through administrative writes in Windows environments or SUDO access for Linux/Unix environments. Log aggregation and monitoring of administrative access is provided through ArcSight SIEM. Reports on access to customer VMs are available for review in the Portal Managed Security Services Tab. There also are access reports within our cloud management system that can be reviewed with customers.
- **Authentication**—CGI uses an Active Directory implementation of LDAP to provide enterprise authentication across the cloud and customer VMs. The same ID is used to access all devices. Authorization is generally handled within the applications that make up our cloud with a few exceptions where the cloud can pull the groups from the Active Directory. Our second factor of authentication uses RSA On-demand Authenticator.
- **Identity management**—CA SiteMinder® is used for identity management. Identities are created, updated or removed using service request forms in the Portal. Each request goes through an approval process where a user group representing the COTR and the ISSO must approve the change prior to implementation. Customers are responsible for reviewing credentials on a periodic basis and should inform CGI in a timely manner of any changes in user roles or permissions.
- **Federated identity management integration**—CGI can establish a one way trust with a customer's LDAP solution to import users into our directory. Analysis is needed to determine whether all directory attributes can be populated, how users would be placed into necessary groups, and how RSA accounts could be provisioned.
- **Application programming interfaces (APIs)**—CGI's Federal Cloud IaaS exposes LDAP APIs for authentication to our Active Directory domain. VMs are joined to the domain when created. Our service request system supports API calls through which requests can be made to create, update or remove users.



## Encryption of Data—Rest/Transit

CGI gives customers the option to selectively encrypt local drives on their VM by leveraging the FIPS 140-2 AES encryption algorithm built into the OS. By allowing customers to do encryption themselves, CGI avoids having identical keys shared across customers. CGI encrypts data on back-up tapes using a FIPS 140-2 AES encryption that are algorithm and transports tapes to a NARA-compliant offsite storage using a secure transport vendor.

Data transmission within CGI's control, such as access to the Portal or through VPNs, is encrypted. Customers are able to configure their own firewalls and are responsible for ensuring their data is properly encrypted when it leaves the cloud. Within the cloud, we isolate customer data files onto their own Logical Unit Numbers (LUNs) and do not permit guest access to the underlying storage.

- *Data at rest*—CGI provides customers with the capability to encrypt data at rest. Instructions for encrypting data are found in the knowledgebase on the Portal Service Management Tab.
- *Data in transit*—CGI requires the use of an SSL VPN connection for access to the Portal and for remote access to VM operating systems.

## Managed Security Services

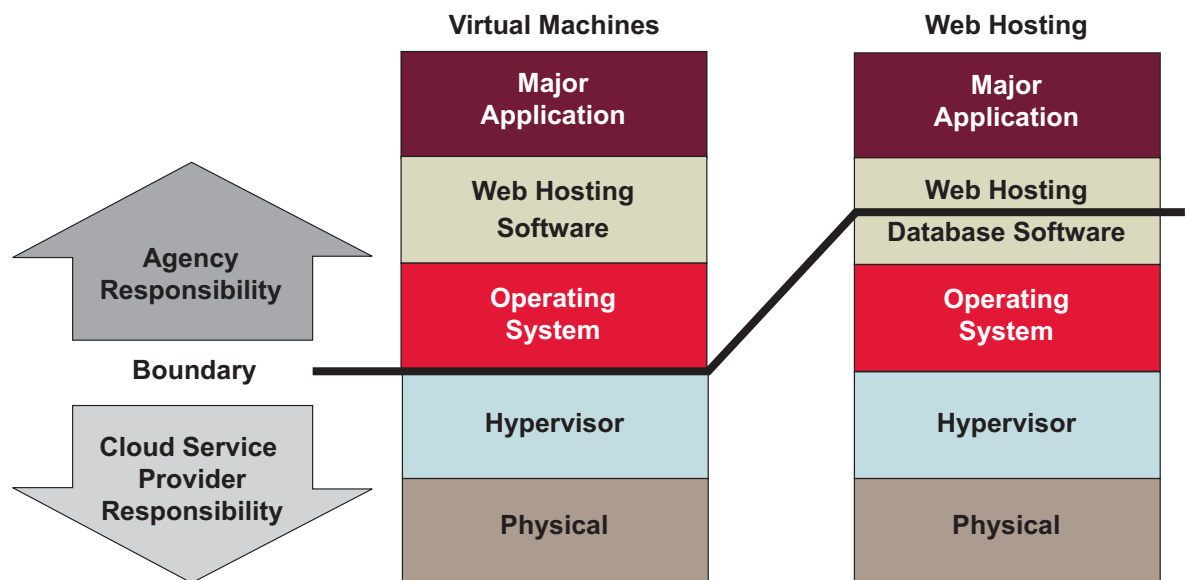
CGI's Managed Security Services tool tracks, defends and reports the security status of compute resources. This includes output from the sentinel and defense systems resident in the hardened environment of the CGI Federal Cloud. The tool enables early discovery of vulnerabilities (for Lot 3: Web Hosting) through deep insights into OS, application and database scan results.

## CGI and Customer Security Responsibilities

Figure 1 shows the security responsibility boundaries between agencies and CGI for VMs and Web Hosting. Agencies are responsible for securing their system. For Web Hosting, CGI handles the OS-related security and a portion of the hosting software security depending upon what has been purchased from CGI. Any responsibility gaps can be identified clearly so that agencies can decide what additional security controls, performance reporting or other standards of compliance are needed, and whether to address those internally or through CGI under GSA IT Schedule 70.

Agency customers are responsible for securing the applications they use to expose their data. This may include certifications, public/private keys, multilayer authentication, etc. Agency customers can also use their Active Directory sub-domain in CGI's cloud to provide authentication and authorization for the file systems.

**Figure 1: Comparison of Agency and CGI Responsibilities**



## Information services for predictable and sustainable savings

CGI's cloud reduces total cost of ownership through a combination of economies of scale, elasticity, automated service management, cost avoidance and ongoing technology investments. CGI's information and reporting services provide the insights agencies need to monitor and manage their usage and costs.

The screenshot displays the CGI Information Portal interface. At the top, the CGI logo and tagline "\_experience the commitment™" are visible. Below this, a navigation bar includes tabs for "VIRTUAL MACHINE MANAGEMENT", "SERVICE MANAGEMENT", "INFORMATION PORTAL", and "MANAGED SECURITY SERVICES". The "INFORMATION PORTAL" tab is active, showing a sidebar with links to "Virtual Machine Management", "Service Management", "Information Portal", and "Managed Security Services". The main content area features a "BPA Invoice" for the month of March, 2011, with BPA Number: GS00Q11AEA0005. The invoice details include the CGI logo, company name "CGI Federal, Inc.", address "12001 Fair Lakes Circle, Fairfax, Virginia 22033", and submission information. A "Summary Invoice" table is also present, showing usage metrics for various services.

Lot #2	Lot Description	CLIN #	CLIN Description	Quantity	Unit	Dollar Amount
0004AA	Windows 2008 with WebLogic	0004AA	Windows 2008 with WebLogic	4	VMs	\$50,000.00
0008BB	Windows 2008 with WebLogic	0008BB	Windows 2008 with WebLogic	3	VMs	\$60,000.00
0014BA	Storage	0014BA	Storage	100	GB	\$10,000.00

## Billing

CGI collects data on a weekly basis and presents billing usage and charges to customers on a weekly basis using a variety of tools via the Portal Information Tab. The CMDB collects information about the provisioned services. Change records in the change management systems provide information about usage of VMs and Web Hosting servers. Monitors provide utilization metrics for data I/O, storage and tape backup.

Bills are rendered monthly in paper or CSV format. Customers can view the status of monthly invoices (billed charges) and view the detailed charges and associated usage metrics on the Portal Information Tab.

## Threshold Notification

Customer Administrators can configure a monthly dollar limit for each Task Order. CGI monitors orders and utilization and, when a threshold of 80 percent of the monthly amount is exceeded, we post a notification on the Portal Information Tab for the Customer Administrator and send an e-mail to the address specified in the Administrator's profile. *Note: Should the customer's monthly invoice reach the monthly dollar amount limit, we will not invoice above the limit, and we will follow agency instructions for handling ongoing service delivery to that customer.*

## Performance and Utilization Monitoring

CGI's Web Hosting bundle includes the following performance utilization and monitoring capabilities provided via the Portal Information Tab:

- Automated Monitoring
  - CPU Utilization
  - Memory Utilization
  - Disk Utilization
  - Network Bandwidth Utilization (data transfer)
  - Disk I/O
- Server Instance Operational Status
  - Pending
  - Provisioning
  - Powered On
  - Powered Off
  - Errors

Simple Network Management Protocol (SNMP) can be configured by the customer on any VMs provisioned, but this capability is not enabled by default. CGI monitors our Web Hosting services using BMC ProactiveNet monitoring. If desired, CGI can provide SNMP traps to customers from our monitoring solution specifically for Web Hosting services.

Customers may leverage their own IP/SNMP-based monitoring tools on their services. As a best practice, CGI recommends deploying the monitoring tool or a proxy within the customer's cloud environment and then aggregating the alerts back to the customer's centralized console. When monitoring tools are used over the Internet, timeouts can occur that can lead to false alerts.

## Trending and Reporting Capabilities

As a standard part of CGI's Federal Cloud IaaS, we provide the monthly management reports listed in Table 3.

**TABLE 3: Monthly Management Reports**

Report / Deliverable	Description	Delivered To	Frequency
<b>Service Level Agreement</b>	<ul style="list-style-type: none"> <li>• Service Availability (Measured as Total Uptime Hours/Total Hours within the Month) displayed as a percentage of availability up to one-tenth of a percent (e.g., 99.5%)</li> <li>• Text description of major outages (including description of root-cause and fix) resulting in greater than one (1) hour of unscheduled downtime within a month</li> </ul>	Ordering Activity COTR	Monthly
<b>Help Desk/ Trouble Tickets</b>	<ul style="list-style-type: none"> <li>• Number of Help Desk/customer service requests received</li> <li>• Number of Trouble Tickets Opened</li> <li>• Number of Trouble Tickets closed</li> <li>• Average mean time to respond to Trouble Tickets (time between Trouble Ticket opened and the first contact with customer)</li> <li>• Average mean time to resolve Trouble Ticket</li> </ul>	Ordering Activity COTR	Monthly
<b>Cloud-Report of Sales</b>	<ul style="list-style-type: none"> <li>• Quantity and type of IaaS service orders received</li> <li>• Number of service orders (and percentage of orders out of the total) which resulted in an e-mail or contact with customer within two (2) hours of individual task order(s) issued under this BPA being sent to vendor</li> </ul>	Designated CO	Monthly
<b>Service Utilization</b>	<ul style="list-style-type: none"> <li>• Monthly utilization of each IaaS Service type (Lot) as defined by the Service Units for the specific offering by the vendor</li> </ul>	Designated CO	Monthly
<b>Invoicing/ Billing</b>	<ul style="list-style-type: none"> <li>• Standard invoicing/billing</li> </ul>	Ordering Activity COTR	Monthly

Custom reports can also be created from data stored in our management tools which include:

- Performance management system
- CMDB
- Incident system
- Change management system

Available reporting levels include aggregate level across agency, program organization and several sub categories.

Delivery can be online, via readable and CSV formats in the Portal Information Tab, or via print reports to the ordering activity COTR. Reports and associated source data will be retained for one year.

### **Event Tracking and Audit Controls**

The combination of user name, password and permissions is the mechanism by which server hosts authenticate a user for access and authorize the user to perform activities. Users can be assigned to groups with a common set of rules and permissions for easier management. Default and custom roles enable pre-defined sets of permissions. Actions initiated by users with the Administrator role are recorded in event logs, providing an audit trail to improve accountability among the Administrator users. Event logs are available online for up to one (1) year.

## **Additional Services Available Under GSA IT Schedule 70**

CGI understands that the needs of federal agencies vary, and we offer a number of ways to customize our Federal Cloud IaaS service offerings through the use of GSA IT Schedule 70.

### **Transition and Migration Services**

Transition is a key phase of CGI's operating framework that is used to help customers get ready to move to the cloud with:

- A well-defined project with a plan that is approved by the customer
- A clearly defined beginning and end, with key acceptances by the customer
- A project manager from CGI who is discrete from the service delivery staff
- A well-defined Knowledge Acquisition/Knowledge Transfer plan

CGI can help agencies:

- Transition current infrastructure, applications and other services into the cloud
- Migrate legacy applications to cloud platforms and make them "cloud aware" to take advantage of elasticity benefits
- Spread migration/transformation costs over the life of the service to eliminate upfront costs and reduce cost of ownership for the transition.

## Proof of Concept/Roadmap

CGI can create proofs of concept to help agencies:

- Determine system requirements to support application instances in the cloud
- Determine load levels of “normal” usage and “peak” demands to evaluate performance of each application instance
- Design and implement service in the cloud leveraging APIs and scripting to automate the provisioning of additional cloud resources as increased application utilization occurs
- Examine licensing models needed to support the application in the cloud
- Perform application/system testing
- Document next steps/lessons learned.

## Security Advisory Services

CGI helps protect operations at the infrastructure and data layers and provides advisory services designed to assess and strengthen security strategies. We offer the full range of security services, including security governance and engineering, cybersecurity and managed security services (e.g., program, configuration, incident and event management and business continuity services).

## For more information

For more information on CGI’s Federal Cloud IaaS offering, please visit <http://www.cgi.com/federalcloud>.

### CGI Federal Cloud Infrastructure as a Service Offering Description

Version Number 4

CGI regularly updates the content of this offering description to provide clarifications and/or additional information of interest to customers.



12601 Fair Lakes Circle  
Fairfax, VA 22033  
USA  
Phone: 703-227-6000