(U) Intelligence Community   
Commercial Cloud Enterprise (IC C2E)

(U) Technical Publishing Guide for AWS Marketplace for the U.S. Intelligence Community

Submission date: April 19, 2022

Table of Contents

[1.0 Abstract 1](#_Toc95221553)

[2.0 Introduction 1](#_Toc95221554)

[3.0 AWS Shared Responsibility Model 1](#_Toc95221555)

[4.0 Building AMIs for AWS IC Marketplace 2](#_Toc95221556)

[4.1 What is an AMI? 2](#_Toc95221557)

[4.2 General Best Practices 3](#_Toc95221558)

[4.3 Specific Requirements for IC Marketplace Products 3](#_Toc95221559)

[4.4 AMI Sharing with IC Marketplace 8](#_Toc95221560)

[4.5 AMI Cloning and Product Code Assignment 10](#_Toc95221561)

[4.6 Clusters and AWS Resources (CAR) 10](#_Toc95221562)

[4.7 Software as a Service Listings 11](#_Toc95221563)

[4.8 Bring Your Own License (BYOL) Listings 11](#_Toc95221564)

[5.0 Providing Product Updates 11](#_Toc95221565)

[5.1 Updating Product Listing Details 11](#_Toc95221566)

[5.2 Publishing a New Version of your AMI 11](#_Toc95221567)

[6.0 Providing Support 12](#_Toc95221568)

[7.0 IC Marketplace Private Offers 12](#_Toc95221569)

[7.1 Security Guidance for IC Marketplace AMI Developers 13](#_Toc95221570)

[8.0 Additional Resources – Links 14](#_Toc95221571)

[8.1 Building AMIs 14](#_Toc95221572)

[8.2 AWS Resources 15](#_Toc95221573)

[8.3 How-to Guides 15](#_Toc95221574)

[8.4 Mistakes to Avoid 15](#_Toc95221575)

[8.5 General 15](#_Toc95221576)

[8.6 Federal Security Guidelines 15](#_Toc95221577)

[9.0 Additional Resources – Documents 15](#_Toc95221578)

[9.1 AWS and IC Marketplace 15](#_Toc95221579)

# Abstract

This document provides information for building, delivering, and maintaining software applications within the AWS Marketplace for the U.S. Intelligence Community (IC), referred to within this document as IC Marketplace. This document should be read as an addendum to the [AWS Marketplace Seller Guide](https://docs.aws.amazon.com/marketplace/latest/userguide/what-is-marketplace.html). It includes specific details, specifications, and examples relevant to listing products within IC Marketplace. All independent software vendors (ISVs), sellers, publishers, vendors, and partners must meet or exceed these specifications for all products.

# Introduction

IC Marketplace is an isolated and distinct implementation of AWS Marketplace. IC Marketplace delivers AWS Marketplace functions and operational capabilities within the Commercial Cloud Services (C2S) program’s scope and objectives, to include providing commercial cloud capabilities and commercial service parity to the IC The IC Marketplace operates within a separate and distinct air-gapped C2S IT infrastructure environment for classified workloads. Products listed on IC Marketplace are licensed for deployment and use by IC accounts operating within the C2S infrastructure. Only software provided by sellers who have received Foreign Ownership, Control, or Influence (FOCI) approval is eligible to be listed on the IC Marketplace.

# AWS Shared Responsibility Model

While AWS manages security of the cloud, security in the cloud is the responsibility of the customer. Customers retain control of what security they choose to implement to protect their own content, platform, applications, systems, and networks, no differently than they would for applications in an on-site data center.

In the AWS Top Secret Region, AWS is responsible for securing and accrediting the underlying infrastructure with Intelligence Community Directive (ICD) 503 (the U.S. IC directive that specifies required security of a system, based on the same National Institute of Standards and Technology [NIST] Special Publication [SP] 800-53 controls as FedRAMP) that supports the cloud, and the AWS customer is responsible for anything they put in the cloud or connect to the cloud. This shared responsibility model can reduce the operational burden for the customer in many ways, and in some cases may even improve their default security posture without additional action on their part. [**Figure 1**](#Figure1) depicts the roles and responsibilities of both parties with respect to security.

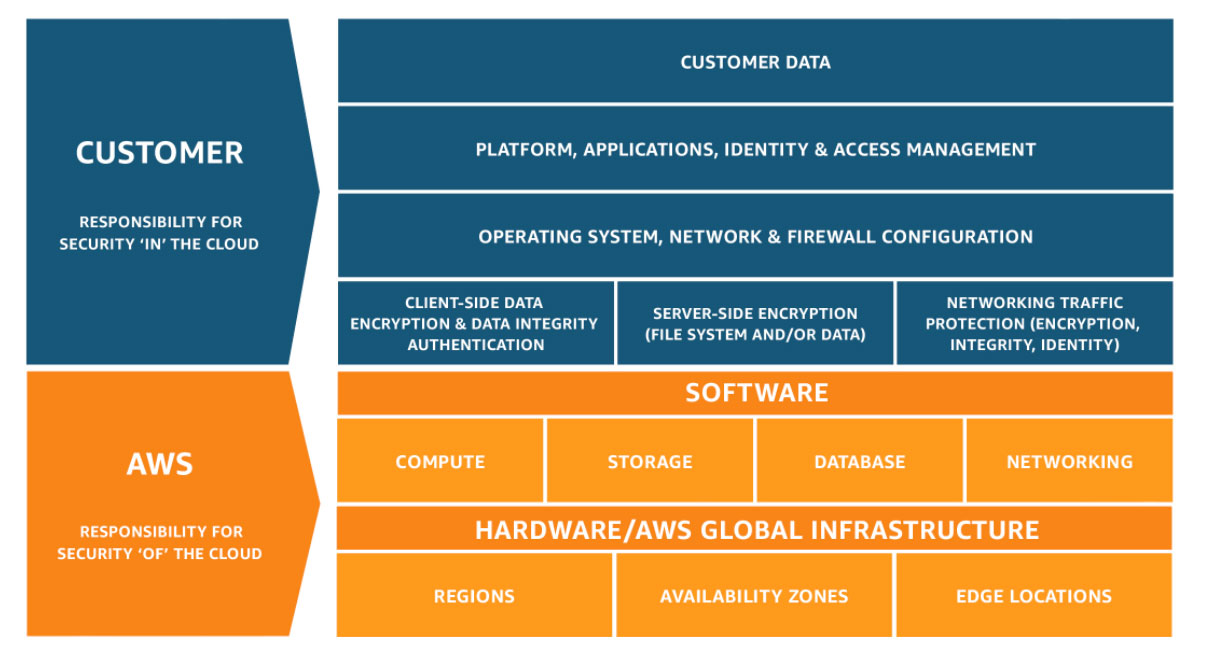


Figure 1: AWS Shared Security Responsibility Model

The amount of security configuration work that the customer must do varies depending on which services they select and the sensitivity of their data. AWS cannot explicitly articulate specific customer security requirements for customer usage, configuration, and security accreditation but will work with IC Marketplace vendors to assist them through the process. However, there are certain security features—such as individual user accounts and credentials, Secure Sockets Layer (SSL)/Transport Layer Security (TLS) for data transmissions, and user activity logging that vendors should configure no matter which AWS Cloud service the customer uses. For more information about these security features, see the “Additional Resources” section at the end of this document.

# Building AMIs for AWS IC Marketplace

## What is an AMI?

An Amazon Machine Image (AMI) provides the information required to launch an Amazon Elastic Compute Cloud (Amazon EC2) instance, which is a virtual server in the cloud. Each IC Marketplace offering contains an AMI that is launched automatically during the subscription process.

An AMI includes the following:

* A template for the root volume of the instance (e.g., an operating system, an application server, and applications);
* Launch permissions that control which AWS accounts can use the AMI to launch instances; and
* A block device mapping that specifies the volumes to attach to the instance when it is launched.

## General Best Practices

The following list of specific requirements for IC Marketplace products are an addendum to the [Best practices for building AMIs](https://docs.aws.amazon.com/marketplace/latest/userguide/best-practices-for-building-your-amis.html) within the [AWS Marketplace Seller Guide](https://docs.aws.amazon.com/marketplace/latest/userguide/what-is-marketplace.html), which should be applied as well.

## Specific Requirements for IC Marketplace Products

### Product Functionality Without the Internet

**The IC Marketplace is not connected to the internet (i.e., the environment is air-gapped). Any attempts by your software to call internet services will fail testing due to lack of connectivity to services outside the air-gapped network.** IC Marketplace products must still be fully functional despite this significant difference from the commercial AWS Marketplace, and software vendors are responsible for validating prior to submission to AWS that the product will still function once published to the air-gapped AWS Top Secret Region. Publishers in IC Marketplace have benefited from partnering with AWS Partner Network (APN) Partners that provide AWS Secret and Top Secret region emulation services accessible from the commercial internet. Please contact [icmp@amazon.com](mailto:icmp@amazon.com) for the latest list of AWS region emulation partners.

The following examples may be helpful when determining a test plan for your product.

* **Server-side Internet communication:** IC Marketplace products will not be able to communicate with resources on the public internet. It is important to test product functionality in a simulated air-gapped environment. One method of simulating the air gap is to deploy the product into a private subnet within a virtual private cloud (VPC) and accessing the product via a [bastion host](https://aws.amazon.com/quickstart/architecture/linux-bastion/).
* **Client web browser redirection:** In some cases, server-side code will redirect a customer’s web browser to a resource that is available on the public internet. A customer’s browser could be redirected to hosted resources, such as www.openlayers.org and ajax.googleapis.com. Requests such as this will fail in the air-gapped region because these resources are not available. During testing, be certain to validate that the client browser is not redirected to resources on the public internet.
* **AWS Application Programming Interface (API) Endpoints:** The AWS API endpoints within the AWS Top Secret Region have different addresses from their public counterparts. Product health checks that attempt to contact an AWS public API endpoint will fail.
* **Amazon EC2 Instance Type Availability:** The AWS Top Secret Region contains a subset of the Amazon EC2 instance types available in AWS commercial regions. A listing of available Amazon EC2 instance types is available on the IC Marketplace Product Form available via the AWS Marketplace Management Portal.[[1]](#footnote-1)
* **Amazon EC2 Spot Instances:** [Amazon EC2 Spot Instances](https://aws.amazon.com/ec2/spot/) are not available inside the AWS Top Secret Region.

### C2S Access Portal (CAP)

The C2S customer base uses the C2S Access Portal (CAP) as the Federated Identity Broker integrating existing IC identity, authorization, and access control systems with the AWS Top Secret Region.

CAP provides federated role-based access to the C2S Management Console and C2S APIs (via AWS Security Token Service [AWS STS] temporary credentials) for C2S users and applications ([**Figure 2**](#Figure2)). The CAP uses the IC’s existing X.509 infrastructure with client certificate authentication (Public Key Infrastructure [PKI]) and a federated role-based access control model.

CAP provides a REST API for applications to request AWS STS temporary credentials that can be used to interact with AWS Top Secret Region APIs and services for a particular C2S account and AWS Identity and Access Management (AWS IAM) Role. As part of the IC Marketplace onboarding process, AWS will provide access to the document “CAP Credentials API Primer,” which provides a summary representation of how to use CAP to request temporary credentials for use by your application or appliance.

Use of CAP is summarized as follows.

* Enables Federated Identity Integration of IC PKI identities with the AWS Top Secret Region APIs
* Leverages AWS STS and AWS IAM services
* Provides a REST API that returns a JSON template containing AssumeRoleResult[[2]](#footnote-2) content and optionally CAP-specific information
* CAP-provided AWS STS tokens expire after 60 minutes

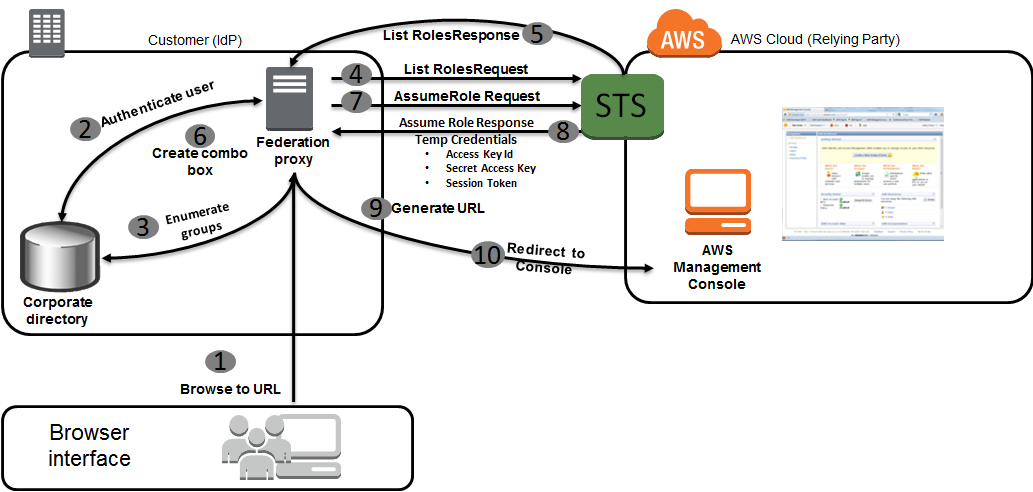


Figure 2: Federated Access to AWS Top Secret Region APIs

* In addition to using CAP credentials, IC Marketplace applications may use AWS IAM Roles for Amazon EC2 in specific cases.[[3]](#footnote-3) The use of AWS IAM Roles for Amazon EC2 is subject to each individual agency’s policy and discretion. Some agencies will not grant an Authority to Operate (ATO) in their production accounts without CAP integration. For other customers, the permissions granted to an AWS IAM Role may not be sufficient for product functionality.
* Most IC Marketplace customers do not have permission to create AWS IAM Roles. AWS IAM Roles need to be created by the agency’s cloud management team and provisioned into the user’s account. IC Marketplace publishers must provide the AWS IAM Role in JSON format as part of their usage instructions.
* IC Marketplace Publishers are permitted to use AWS IAM Roles for Amazon EC2 when the product accesses an AWS (C2S) resource that is within the caller’s AWS (C2S) account AWS IAM security boundary.
* IC Marketplace Publishers are NOT required to use CAP issued credentials when the product issues an API call to a third-party service that is within the caller’s AWS (C2S) account AWS IAM security boundary.
* IC Marketplace Publishers are required to use CAP issued credentials when the product accesses an AWS (C2S) resource that is outside the caller’s AWS (C2S) account AWS IAM security boundary.
* CAP integration testing can be tested using CAP simulation and testing tools, available through commercial vendors. For recommendations, please contact us at [icmp@amazon.com](mailto:icmp@amazon.com).

### Additional Requirements for IC Marketplace Products

* Products **MUST** provide a mechanism to completely disable all attempts to connect to the public internet.
* AMIs provided by publishers **MUST** comply with the AWS Service Terms.[[4]](#footnote-4) For example, Microsoft SQL Server Web edition may not be used inside the air-gapped IC region due to a lack of public internet connectivity.
* Products **MUST** be based on hardware virtual machine (HVM) AMIs.
* Products **MUST NOT** attempt to access any external resources without clearly articulating such a behavior in the product documentation.
* Products **MUST** include a mechanism to add additional Root and Trusted Certificate Authorities to the product Trust Store(s) as well as remove undesired entries from the product Trust Store.
  + Commercial Certificate Authorities, such as DigiCert and Symantec, are not present in the AWS Top Secret Region to provide validation for generally trusted Internet Root Certificate Authorities. The AWS Top Secret Region API endpoint certificates are signed by Certificate Authorities that are specific to the AWS Top Secret Region and are not available on the public internet.
* Products MUST allow the customer to define the network time source as pool.ntp.org and other internet time sources are not available.
* Amazon EC2 Instance Identity Document validation is not required in the AWS Top Secret Region; however, products that require verification of the Amazon EC2 Instance Identity Document via the Amazon EC2 Metadata Service MUST request the AWS Top Secret Region (us-iso-east-1) specific public keys and incorporate them into the product. Requests for the public keys should be made to AWS Support via a customer support case.
* The use of static authenticators (such as Access Key and Secret Access Key) is prohibited for both AWS Marketplace and IC Marketplace products. Several methods of making API calls using temporary credentials are available to IC Marketplace vendors.
* Products MUST do the following to interact directly with AWS Cloud services:
  + Use AWS Signature Version 4 API[[5]](#footnote-5)
  + Use AWS Software Development Kit (SDK) versions released after November 2014 (NOTE: We recommend using the most current General Availability (GA) SDK release.)
  + Allow the customer specification of an alternate AWS SDK endpoint file and certificates using AWS SDK configuration parameters.
  + Support the use of AWS STS[[6]](#footnote-6) or AWS IAM Roles for Amazon EC2 as an alternative to AWS IAM Users.
  + Use of the AWS SDK specific version of the DefaultCredentialProviderChain[[7]](#footnote-7) is the best practice to enable customers to manually provision AWS STS credentials or provide credentials through other means.
* Products **SHOULD** use the Amazon EC2 Instance Metadata Service (IMDS)[[8]](#footnote-8) to derive the region the product is running in and form the AWS API endpoint hostnames[[9]](#footnote-9) using the global endpoint naming standard <service name>.<region>.<services/domain>.
  + ec2.us-east-1.amazonaws.com
  + ec2.us-iso-east-1.<services/domain>

### IC Marketplace Publisher Requirements

* A paid product listing in the commercial AWS Marketplace is a prerequisite for licensing products to AWS for listing in the IC Marketplace. This requirement can be met by having a paid AMI listing in the AWS GovCloud (U.S.) Regions within the AWS Marketplace because AWS GovCloud (U.S.) is a commercial region that hosts sensitive data and regulated workloads, including the most stringent U.S. government security and compliance requirements. Industry case studies for AWS GovCloud (U.S.) can be found on the [AWS GovCloud (U.S.) page.](https://aws.amazon.com/govcloud-us/?whats-new-ess.sort-by=item.additionalFields.postDateTime&whats-new-ess.sort-order=desc)
* IC Marketplace listings of products and services will need to be optimized to conform with IC standards and requirements, including region-specific service endpoints, AWS Cloud service availability in region, publisher support for product security assessments, and compliance with IC security accreditation standards.
* Publishers must agree to disclose and maintain status regarding current FedRAMP assessment and authorization results, if any. Applicable U.S. public sector compliance programs include [ICD 503](http://www.dni.gov/files/documents/ICD/ICD_503.pdf), [FedRAMP](http://cloud.cio.gov/fedramp), [DoD DIACAP](http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf), [DoD Cloud Computing Security Requirements Guide (CC SRG)](http://iase.disa.mil/cloud_security/Pages/index.aspx). Working with the publisher, AWS will assign products to one of four accreditation readiness tiers:
  + Tier 1+: Product has successfully completed an ICD 503 assessment and is authorized to operate in one or more production workloads in the AWS Top Secret Region.
  + Tier 1: Product has successfully completed a major industry or U.S. Public Sector standard accreditation such as ICD 503, FedRAMP, DoD DIACAP, DoD CC SRG. In addition, the software has successfully passed AWS Marketplace security reviews and has a record of safe operations with AWS commercial customers.
  + Tier 2: Software/Service is well into the process of achieving a major industry standard accreditation. In addition, the software has successfully passed AWS Marketplace security reviews and has a record of safe operations with AWS commercial customers.
  + Tier 3: No major industry standard accreditation has been granted or started; however, the software has successfully passed AWS Marketplace security reviews and has a record of safe operations with AWS commercial customers.

Submit your IC Marketplace Product from the AWS Marketplace Management Portal

1. Go to the [Server Product tab](https://aws.amazon.com/marketplace/management/products/server?).
2. Select your commercial product intended for IC Marketplace.
3. Under the Actions menu, download the product load form.
4. Download an [IC Marketplace product load form](https://s3.amazonaws.com/awsmp-loadforms/IC+Marketplace+Product+Load+Form.xlsx).
5. Copy commercial data into the IC Marketplace load form.
6. Note that available instance types are different in IC Marketplace.
7. Use the [File upload tool](https://aws.amazon.com/marketplace/management/product-load?) to submit your IC Marketplace product.

### Timing for Product Submissions

AWS processes requests as quickly as possible. Due to the unique technical characteristics of the air-gapped AWS Top Secret Region, however, the testing and publishing cycle can often require multiple iterations with the software vendor. Adherence to all of the requirements contained in this Technical Publishing Guide will significantly reduce workload by all parties and speed your time to market.

After your initial submission of an AMI and load form, you should expect to hear back from AWS within 7 *business* days. However, loading and testing within IC Marketplace is much more time intensive than for commercial AWS processes, so exact times may vary.

Product availability within IC Marketplace will take a minimum additional 5 business days following product availability in AWS Marketplace. This period is subject to change depending on product complexity, testing results, and concurrent operational workload. If you have any questions about your request, please contact us at [icmp@amazon.com](mailto:icmp@amazon.com) or through your [AWS Marketplace contact form](https://aws.amazon.com/marketplace/management/contact-us/?).

## AMI Sharing with IC Marketplace

AMIs and **all** associated snapshots **MUST** be shared and accessible to the AWS IC Marketplace AMI ingest account (to be provided to IC Marketplace Publisher following government FOCI approval) when an AMI is ready to be processed.

Follow these steps to grant access to the AMI and snapshots.

### AMI and Snapshot Sharing via the AWS Marketplace Management Portal

1. Log into the [AWS Marketplace Management Portal](https://aws.amazon.com/marketplace/management/tour).
2. Once logged into the Management Portal click the “Assets” tab in the top navigation bar and select “Amazon Machine Image.”
3. Click “Share AMIs” and select the AMI(s) you wish to share.
4. Once the AMI is shared you can find it by clicking the “Shared” button.
5. Within the “Shared” view you can see the “Status” of your AMI, which references the results of our security scanning. Initially the status will be “Scanning.” Once the scan is complete it will indicate the status and provide guidance regarding any mediation needed.

### AMI and Snapshot Sharing via the Amazon EC2 Console

1. In the [AWS Management Console](https://signin.aws.amazon.com/), access the Amazon EC2 Dashboard.
2. Click “AMIs” in the left-hand navigation bar.
3. Select the AMI to be shared.
4. Select the Permissions tab at the bottom of the page.
5. Check the box to add “create volume” permissions to the associated snapshots when creating permissions.
6. Click “Edit.”
7. Enter 679593333241 into the text field.
8. Click “Save.”
9. You should see the account number listed under “AWS Account Number.”

To **verify** that the snapshot(s) have been correctly shared:

1. Click “Snapshots” in the left-hand navigation bar.
2. Select the snapshot(s) associated with the AMI.
3. Click “Permissions.”
4. You should see “aws-marketplace” in the list of “Remove Create Volume Permission/.”
5. If you do not see it listed, you can add AWS Account Number <ingest account number> and click “Save/”

### AMI and Snapshot Sharing via the Amazon EC2 Command Line Interface (CLI)

There are multiple methods to share the snapshot(s) of a public AMI (AWS SDKs, AWS Command Line Interface [CLI], Amazon EC2 CLI). The following example uses the Amazon EC2 CLI.

1. Run this command from the command line using the Amazon EC2 CLI tools: ec2-modify-snapshot-attribute <snapshot\_id> -c --add <ingest account number>.
2. Replace <snapshot\_id> with the snapshot ID of the snapshot underlying the AMI. If the AMI uses multiple snapshots, this command should be run for each snapshot.
3. If you are unsure of the snapshot ID you can run ec2-describe-images to see the snapshot ID associated with the AMI on the command line.

## AMI Cloning and Product Code Assignment

Once your AMI is submitted, AWS Marketplace will create cloned AMIs for the AWS Top Secret Region. During this cloning and publishing process, AWS will attach an AWS Marketplace product code to the cloned AMIs. AWS uses the AWS Marketplace product code to meter AMI usage. Your software can query the Amazon EC2 IMDS in order to validate that the product code provided by IMDS matches the product code you expect.[[10]](#footnote-10)

Product codes generated for IC Marketplace AMIs will be different from codes used in the AWS Marketplace. If your software queries the IMDS for product code validation, product updates will be required to account for the IC Marketplace product code. When you initially submit your product to the IC Marketplace be sure to ask the Catalog Operations team to provide the IC Marketplace specific product ID. For more information about AWS Marketplace product codes, contact the [AWS Marketplace Seller and Catalog Operations Team](https://aws.amazon.com/marketplace/management/contact-us/?)

## Clusters and AWS Resources (CAR)

Clusters and AWS Resources (CAR)[[11]](#footnote-11) is an AWS Marketplace feature that allows an application to be represented by up to three [AWS CloudFormation](https://aws.amazon.com/cloudformation/) templates, each created by the application vendor, and each with a distinct set of deployment options. Before a buyer launches a template-backed product, they will see a list of the AWS resources that will be created, along with an estimate of the monthly costs. Vendors also have the option to provide the traditional AMI-powered option alongside the new and more powerful template-powered options.

CAR is available in the AWS Marketplace for the U.S IC. For more information, see the [AWS Marketplace Seller Guide](https://docs.aws.amazon.com/marketplace/latest/userguide/cloudformation.html). This guide contains specific best practices for a clustered deployment. Note that Clusters and AWS Resources with Multiple AMIs (CARMA) is not currently supported in the AWS Top Secret Region. Please reach out to [icmp@amazon.com](mailto:icmp@amazon.com) to discuss how we can support your CARMA product.

In addition to following our addendum, engage the AWS Marketplace Solutions Architecture Team in order to verify that the AWS Cloud services called by your template are available in the AWS Top Secret Region and are at the appropriate version levels for compatibility. Additionally, as covered in the “Federated Access to AWS Top Secret Region APIs” section above, many users in the IC may not have the necessary account permissions to set AWS IAM parameters. As such, we recommend that vendors provide at least one AWS CloudFormation template option that does not leverage AWS IAM and name it accordingly.

## Software as a Service Listings

AWS Marketplace cannot provide ISVs direct access to the AWS Top Secret Region to establish a Software as a Service (SaaS) listing in IC Marketplace. We will be unable to support SaaS product listings in IC Marketplace unless directed by the C2S Sponsor to provide an ISV direct access. If your AWS Marketplace software is delivered using the [SaaS model](https://docs.aws.amazon.com/marketplace/latest/userguide/saas-products.html), the IC Marketplace team can discuss how sellers have delivered their application into the AWS Top Secret Region through IC Marketplace using AMIs and AWS CloudFormation. Reach out to [icmp@amazon.com](mailto:icmp@amazon.com) for more details.

## Bring Your Own License (BYOL) Listings

Section 5 of the Terms and Conditions for AWS Marketplace Sellers provides additional terms for non-paid listings. Specifically, sellers must have a corresponding paid listing in the IC Marketplace no later than 90 days after the initial listing of the non-paid listing version, unless we determine that we cannot accept paid listings from you for regulatory reasons. Given this is a commercial requirement, we will not accept BYOL listings from sellers who are not compliant with the commercial terms and conditions for AWS Marketplace sellers.

# Providing Product Updates

## Updating Product Listing Details

Once your product is listed on AWS Marketplace, you may update the listing by submitting change requests regarding the product name, product description, product pricing, compatibility with Amazon EC2 instance types, product-specific end user license terms (if any), and other details. You record these updates in the [IC Marketplace Product Form](https://s3.amazonaws.com/awsmp-loadforms/IC+Marketplace+Product+Load+Form.xlsx), which is located on the AWS Marketplace Management Portal.[[12]](#footnote-12) Once your updates are complete, you upload the completed form using the same interface within the [AWS Marketplace Management Portal](https://aws.amazon.com/marketplace/management/product-load?).

## Publishing a New Version of your AMI

If you wish to publish a new version or an upgrade of your software, you should submit the new AMI to the AWS Marketplace Team via the Marketplace Management Portal using the IC Marketplace Product Form. When the new version has been published, AWS Marketplace will notify your existing users that the new AMI is available and provide them with your release notes and upgrade instructions.

# Providing Support

The IC Marketplace support model differs from the AWS Marketplace support model. Publishers will provide support phone numbers and email addresses within the Seller Load File. Publishers that provide secured support phone numbers and email addresses can also provide these contacts within the Seller Load File (“Secure Support Contacts” and “Secure Support Description” fields).

When an IC Marketplace customer needs software support, they will file a case with the AWS Enterprise Support Team. The AWS Enterprise Support Team will provide the customer with the publisher’s support email and addresses, as provided through the Seller Load File.

The AWS C2S Access Registration Service allows publishers to establish secure support channels for IC Marketplace customers with AWS holding two clearances for each approved vendor. To participate in the Access Registration Service, publishers must:

* Agree to the AWS IC Marketplace Publisher Addendum to the Terms and Conditions for AWS Marketplace sellers.
* Receive FOCI approval.
* Have at least one paid product in the commercial AWS Marketplace.
* Update IC Marketplace AMIs as necessary to comply with applicable regulatory and compliance requirements.

Publishers with cleared support options are able to provide a better IC Marketplace customer experience. Contact [icmp@amazon.com](mailto:icmp@amazon.com) if you would like additional details on the Access Registration Service.

# IC Marketplace Private Offers

[Private offers](https://docs.aws.amazon.com/marketplace/latest/buyerguide/buyer-private-offers.html) are a purchasing program that allows sellers and buyers to negotiate custom prices and end user licensing agreement terms for software purchases and transact through IC Marketplace. In addition to custom prices, publishers may include firm fixed price services necessary to support or integrate the product into the AWS Top Secret Region. This support shall be included in the subscription or metered pricing listed in the IC Marketplace for any product. Private offers require prior review and approval of each transaction. The IC Marketplace team ([icmp@amazon.com](mailto:icmp@amazon.com)) can provide you additional details on the private offer program.

## Security Guidance for IC Marketplace AMI Developers

As stated previously, this guide is an addition to the [AWS Marketplace Seller Guide](https://docs.aws.amazon.com/marketplace/latest/userguide/what-is-marketplace.html). All of the [AWS security policies](https://docs.aws.amazon.com/marketplace/latest/userguide/product-and-ami-policies.html) outlined there must be met for the IC Marketplace as well.

When developing AMIs for the IC Marketplace you should also consider the use case of the customers you will be serving with the secured region. One or more of the following compliance programs may apply.

### FedRAMP and ICD 503

* [FedRAMP](https://cloud.cio.gov/strategy/" \l "fedramp)
* [ICD 503](https://www.dni.gov/files/documents/ICD/ICD503.pdf)

### NIST SP 800-53 Control Compliance

* [NIST SP 800-53, Revision 4](http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf)

### Support and Documentation

* Provide install and deployment guidance in a format that can be migrated to the AWS Top Secret Region.
* Include sufficient details for users to self-serve given that they may not be able to contact your team for additional support.

### Publicity

We encourage you to announce your product’s availability on the AWS Marketplace for the IC; however, all public content such as press releases, blog posts, and marketing collateral that references the I.C. and/or AWS Marketplace for the IC **MUST** be reviewed and signed off by AWS before any publication or announcement is made. While we encourage you to make announcements after AWS approval, we cannot support joint press releases with IC Marketplace publishers. We will, on a per case review basis, support press releases with a quote from AWS if it meets several conditions, including, but not limited to, announcing a new product or service listed on the AWS Marketplace for the IC or including a government-approved customer reference that uses the AWS Marketplace for the IC As stated in Section 7.1 of the AWS IC Marketplace Publisher Addendum, violations of this directive constitute a material breach of the agreement, and the publisher’s IC Marketplace listing may be immediately terminated without notice.

All third-party press releases must be drafted by you (the publisher). We suggest the following headline: “[Insert product name] Now Available on the AWS Marketplace for the U.S. Intelligence Community.” Please use the messaging in this document for consistency.

The press release **should:**

* Clearly and accurately describe how the announcement relates to AWS.
* Clarify the publisher’s role on AWS and with customers.
* Be customer-focused and emphasize customer benefits.
* Use the approved IC Marketplace description: The AWS Marketplace for the U.S. IC is a private community cloud supporting the Intelligence Community. The AWS Marketplace for the IC disrupts traditional methods for trying and procuring software by eliminating the need for individual contract negotiations for software. The AWS Marketplace for the IC provides another solution for the Intelligence Community in their existing toolkit of AWS resources: AWS’s community cloud for application hosting, storage, and data analytic services.

The press release **should not:**

* Specifically identify or infer product use by members of the IC You may only state that your product is available for use on the AWS Marketplace for the U.S. IC
* Specifically identify or infer your product’s use in a mission, use case, or operational applications specific to the IC For example:
  + You **CAN SAY** that your product is used “to process geospatial data and is available in the AWS Marketplace for the U.S. IC”
  + You **CANNOT SAY** that your product is used “by Agency X to process geospatial data concerning Mission Y.”
  + You **CAN SAY** that your product is “used in natural language processing, specifically focused on the following languages… and that your product is available in the AWS Marketplace for the U.S. I.C.”
  + You **CANNOT SAY** that your product is “being used by Agency X for natural language processing to process the following languages.”
* Include a quote from an IC member representative or IC support contractor.
* Include any sales projections, sales actuals, or product consumption metrics in reference to a specific member or subset of the IC.
* Refer to your organization as an associate or partner of Amazon.com because this could be confused with Amazon Associates, our online affiliate program.
* Disclose proprietary information about how your product is integrated/applied, where, how often, at what capacity, or for what purpose your product is being used within the IC.

# Additional Resources – Links

## Building AMIs

* [Creating Your Own AMIs](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/creating-an-ami.html)
* [Sharing AMIs Safely](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AESDG-chapter-sharingamis.html)
* [Using Amazon EBS-Backed AMIs and Instances](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html)

## AWS Resources

* [AWS Security Center](http://aws.amazon.com/security/)
* [AWS Penetration Testing](http://aws.amazon.com/security/penetration-testing/) (includes a penetration testing request form for public regions)
* [AWS Security Best Practices whitepaper](https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf)
* [AWS Overview of Security Processes whitepaper](https://d1.awsstatic.com/whitepapers/aws-security-whitepaper.pdf)

## How-to Guides

* [The Center for Internet Security (CIS): Security Benchmarks](http://benchmarks.cisecurity.org/downloads/benchmarks/)
* [The Open Web Application Security Project (OWASP): Secure Coding Practices Quick Reference Guide](https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide)

## Mistakes to Avoid

* [OWASP Top 10 Web Application Security Risks](https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project)
* [Common Weakness Enumeration](https://cwe.mitre.org)

## General

* [Linux Forums](https://www.linux.org/forums/)
* [NIST National Vulnerability Database](http://nvd.nist.gov/)

## Federal Security Guidelines

* [FedRAMP](https://cloud.cio.gov/strategy/" \l "fedramp)
* [NIST SP 800-53, Revision 5](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5-draft.pdf)
* [ICD 503](http://www.dni.gov/files/documents/ICD/ICD_503.pdf)

# Additional Resources – Documents

## AWS and IC Marketplace

* [AWS Marketplace Seller Guide](https://docs.aws.amazon.com/marketplace/latest/userguide/what-is-marketplace.html)
* C2S Access Portal Credentials API Primer (provided in the IC Marketplace intro packet, available on request)

1. <https://aws.amazon.com/marketplace/management/> [↑](#footnote-ref-1)
2. <http://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRole.html> [↑](#footnote-ref-2)
3. <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html> [↑](#footnote-ref-3)
4. <https://aws.amazon.com/service-terms/> [↑](#footnote-ref-4)
5. <http://docs.aws.amazon.com/general/latest/gr/signature-version-4.html> [↑](#footnote-ref-5)
6. <http://docs.aws.amazon.com/STS/latest/UsingSTS/Welcome.html> [↑](#footnote-ref-6)
7. <http://docs.aws.amazon.com/AWSSdkDocsJava/latest/DeveloperGuide/credentials.html> [↑](#footnote-ref-7)
8. <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html> [↑](#footnote-ref-8)
9. <http://docs.aws.amazon.com/general/latest/gr/rande.html> [↑](#footnote-ref-9)
10. <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/paid-amis.html#get-product-code> [↑](#footnote-ref-10)
11. <https://aws.amazon.com/blogs/aws/new-aws-marketplace-support-for-clusters-and-aws-resources/> [↑](#footnote-ref-11)
12. <https://aws.amazon.com/marketplace/management/> [↑](#footnote-ref-12)