IT Security Procedural Guide: Federalist Site Review and Approval Process CIO-IT Security-20-106

Initial Version

April 13, 2020

Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Initial Release – April 13, 2020		
N/A	Agosto, Dean, Klemens	New guide.	Guide needed to document the process required for sites to be approved for the Federalist platform.	N/A

Approval

IT Security Procedural Guide: Federalist Site Review and Approval Process, CIO-IT Security 20-106, Initial Version, is hereby approved for distribution.

X DocuSigned by:
Bo Berlas
FD717926161544F...

Bo Berlas
GSA Chief Information Security Officer

Contact: GSA Office of the Chief Information Security Officer (OCISO), Policy and Compliance Division (ISP) at ispcompliance@gsa.gov.

Table of Contents

Note: It may be necessary to copy and paste hyperlinks in this document (Right-Click, Select Copy Hyperlink) directly into a web browser rather than using Ctrl-Click to access them within the document.

1 Introduction

Federalist is a General Services Administration (GSA) platform providing software-as-a-service for self-service publishing and maintenance of static web pages. Users are provided with customizable templates for common website use cases. Federalist is hosted on the cloud.gov Platform as a Service (PaaS) and leverages the cloud.gov Agency FedRAMP ATO to provide user sites in an S3 bucket brokered by cloud.gov.

By leveraging cloud.gov, Federalist inherits a portion of the operational challenges as cloud.gov operates, manages, and controls portions or all of the platform components ranging from the Virtual Private Cloud (VPC) and Infrastructure Services all the way down to the physical security of the facilities in which the PaaS services operate.

1.1 Purpose

The purpose of this guide is to define GSA's process for reviewing the security status of sites requesting to be on-boarded to the Federalist platform and approving the site for hosting.

1.2 Scope

The requirements outlined within this guide apply to and must be followed by all Federal employees and contractors who are involved in the process of obtaining approval for sites to be hosted on the Federalist platform.

1.3 Policy

GSA CIO Order 2100.1, "*GSA Information Technology (IT) Security Policy*" states in Chapter 3, Section 2.k:

"All information systems must be authorized, in writing, before they go into operation. The authorization must be IAW one of the A&A processes in GSA CIO-IT Security-06-30 which requires the system and its risks to be assessed and reported in A&A/ATO packages. The A&A/ATO packages, and therefore system risks, must be updated IAW the system's specific A&A process schedule."

2 GSA Federalist Review and Approval Methodology

The following sections describe the review and approval process for static sites requesting to be hosted on the GSA Federalist Platform. The process requires the completion of a Federalist Site Review and Approval Template which is available on the GSA IT Security Forms page.

2.1 Site Information

The requestor must complete Section 1, Site Information, in the template with the following information. A brief description is provided, where necessary to provide details on the required information.

- Site Organization
- Site Name
- Amazon S3 Bucket Name
- Proxy URL
- CloudFront Distribution
- Site URL
- Leveraged Authorizations - include the Information System Name, Service Provider Owner, and the Date ATO Granted for any authorizations the site leverages. Note: The template lists the standard ATOs for Federalist.
- Site Description - Provide a brief description of the site, its purpose, its content, and its use.
- Provide answers to the following questions in the template and follow the instructions in the template, as necessary, based on the answer.
    - Is the site limited to static content only?
    - Is the FIPS 199 impact level of the data Low?
    - Does the Site integrate with any third party resources? – A third party site integration table will need to be completed for all site integrations. The table provides an overview of the third party resource used, including the type of data and the risk level based on the sensitivity of the data, authentication of users and use of MFA, access controls, auditing capabilities, encryption of data, and the connections to the third party site. This data will be used to assess the overall risk of integrating with the third party resource.
      Note: Static website hosting on the Federalist platform is specific to static webpages with no dynamic content or third party integration. Static webpages that do not conform must specifically be reviewed and approved by the GSA Information System Security Officer (ISSO), Information System Security Manager (ISSM) and Chief Information Security Officer (CISO) for hosting consideration on Federalist.
    - Does the Site integrate with any AWS Services beyond S3, WAF, CloudFront, and Shield/Shield Advanced? – A table will need be completed identifying any additional AWS services used.

2.2 High Level Architecture

A diagram of the high level site architecture must be included in the template.

2.3 Binding Operational Directive (BOD) 18-01 Checks

Department of Homeland Security BOD 18-01 requires specific email and web configuration settings. Complete this section regarding the status of the configuration settings required by BOD 18-01. For reference see this link, BOD 18-01.

2.4 Site S3 Bucket Configuration

Document detailed Site S3 Bucket configuration data ensuring bucket permissions are limited to minimal requirements. Screenshots of the configuration settings must be provided.

2.5 Site CloudFront Configuration

Document detailed CloudFront configuration data (e.g. distribution id, distribution status, domain name, etc.), ensuring CloudFront configuration is limited to what is minimally required. Screenshots of the configuration settings must be provided.

2.5.1 CloudFront Connection Limits

Identify the connections limits for the site.

2.5.2 Geolocation Restrictions by Country

Identify the connections limits for the site. List any geolocation restrictions enforced for the site. Typical GSA restrictions are listed in the template for consideration.

2.6 Site AWS Web Application Firewall Configuration

Document detailed AWS WAF configurations for the site. Note: AWS WAF is required only if other than static only content is rendered. Screenshots of configuration settings must be provided when applicable.

2.7 Site Shield/Shield Advanced Configuration

Document detailed AWS Shield and Shield Advanced configurations. Screenshots of Site Shield/Shield Advanced configuration settings must be provided.

2.8 Site Web Vulnerability Scanning

Document the following elements in the template:

- Scan URL
- Scan Tool
- Authenticated or Not
- Scan Completed or Not
- Date of Scan
- Populate the Scan Summary Table with the number of Critical, High, Moderate and Low findings, both originally found and current.

- Populate the Scan Findings table with the details listed in the template for all Moderate, High, and Critical findings.
- Provide a link to Site Web Vulnerability Scan Report.

2.9 Site Static Code Scanning

Document the following elements in the template:

- Code Repo URL or Link to Code Attachment
- Scan Tool
- Scan Completed or Not
- Date of Scan
- Populate the Scan Summary Table with the number of Critical, High, Moderate and Low findings, both originally found and current.
- Populate the Scan Findings table with the details listed in the template for all Moderate, High, and Critical findings.
- Provide a link to the Code Scan Report.

2.10 Approval Process

The ISSO and Site Owner collaborate to complete the Federalist Site Review and Approval Template. Once completed the ISSM reviews and approves the site for hosting or coordinates with the ISSO and Site Owner on any issues regarding the site.

3 Maintaining Approved Sites

Sites hosted on Federalist are required to have the URLs scanned in accordance with CIO-IT Security-06-30, "*Managing Enterprise Risk*," and GSA's parameter for National Institute of Standards and Technology (NIST) Special Publication Control RA-5, Vulnerability Scanning.

Any changes to the hosted site must be evaluated by the ISSO to determine if there is a security impact and/or if the approval template needs to be updated and re-signed.