IT Security Procedural Guide: General Services Administration (GSA) Pages Site Review and Approval Process CIO-IT Security-20-106

Revision 2

March 11, 2024

U.S. General Services Administration

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
		Revision 1 – March 29, 2023		
1	Klemens	• No new agreements to host sites on Federalist will be permitted after April 1, 2023. However, Section 3, Maintaining Approved Sites, still will be enforced. Therefore, this guide is being reissued without technical change. • Minor editorial updates were made where necessary and to maintain 508 compliancy.	Reissue guide to align it with guide update frequency.	Throughout
		Revision 2 – February 23, 2024		
	Jediny, Frederick, Klemens	• Renamed guide and updated the process to align with GSA's Implementation of Cloud.gov Pages' Authorization to Operate. • Added sections on reassessment and the consequences of failing to maintain sites.	Updated to reflect new GSA guidance.	Throughout

Approval

IT Security Procedural Guide: GSA Pages Site Review and Approval Process, CIO-IT Security 20-106, Revision 2, is approved for distribution.

DocuSigned by:
Bo Berlas
FD7170261615144F...

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

1 Introduction

GSA Pages 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. GSA Pages 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, GSA Pages 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 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 GSA Pages 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 GSA Pages platform.

1.3 Policy

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

> *All information systems must be authorized, in writing, before they go into operation. The authorization must be in accordance with (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 Pages Review and Approval Methodology

The following sections describe the review and approval process for static sites requesting to be hosted on the GSA Pages platform. The process requires the completion of a GSA Pages Site Review and Approval Template, which is available on the GSA IT Security Forms and Aids page. It will be referred to as the Template in the remainder of this guide.

2.1 Site Information

The GSA Website Manager must complete the Google Form for GSA Website Managers to provide information about the website. Additional instructions regarding the required information are provided within the Template.

Site Information:

GSA Site Organization:

Site Name:

Amazon S3 Bucket Name:

Preview URL:

Site Public URL:

Site Github Repository URL:

Leveraged Authorizations:	Include the Information System Name, Service Provider Owner, and the Date ATO Granted for any authorizations the site leverages. (Note: The form template lists the standard ATOs for GSA Pages.)
Site Description:	Provide a brief description of the site, its purpose, its content, and its use.

Note: The Template provides selections or additional information and guidance when answering the questions listed throughout this guide.

- Is the site a stand alone or part of another FISMA system?
- If part of another FISMA system, which system?
- Is the site limited to static content only?
- Is the FIPS 199 impact level of the data Low?

2.2 GSA Digital Lifecycle Program

All Sites are required to participate in GSA's Digital Lifecycle Program and complete a Digital Lifecycle Spreadsheet.

2.3 Integrations

If the GSA Pages site integrates with third party or AWS resources, scripts, or services, instructions for providing information about the integrations are included in the Template. The following subsections provide an overview of the various types of integrations.

2.3.1 Third Party Integrations

Does the Site integrate with any third party resources?

The Template provides the following list of third party integrations that have already been documented. In the form they can be selected by marking checkboxes next to the third party resource.

- Search.gov
- Digital Analytics Program (DAP)
- Touchpoints
- Google Analytics
- Google Tag Management
- ZenDesk
- GovDelivery
- Netlify CMS

2.3.2 Other Third Party Javascript or Integrations

For all other third party integrations a table (see Table 2-1) will need to be completed providing details about the integration. This data will be used to assess the overall risk of integrating with the third party resource.

Table 2-1. Other Third Party Integration Details

Third Party Site Integration	Details on the Integration
System Name	
Connection Type	
Data Description	
Data Sensitivity	
Level of Vendor Dependency	
Alternative Exists	
Is API over HTTPS?	
API Connection Security	
API Connection Type	
Authentication and Authorization	
MFA	
Role-based Access Control	
Audit Logs Available	
Encryption in Transit	
Encryption in Storage	

2.3.3 AWS Integrations

For AWS services integrated with the site, the standard services must be identified and details on additional services must be documented.

Standard AWS services are:

- WAF
- Shield/Shield Advanced

For additional AWS services information about its use must be provided in a table (see Table 2-2. Additional AWS services may preclude hosting on the GSA Pages platform.

Table 2-2. Additional AWS Services

AWS Service Name	Service Function	How is it being used?

2.6 TTS Technical Operations Team Information

The TTS Technical Operations Team will collect, verify, and provide information regarding the following items in the Template.

Continuous Code Scanning

Link to Code Scanning screenshot:

Link to Dependabot screenshot:

Link to Site Enabled in Allstar screenshot:

Link to Github Repository Security screenshot:

Github Personnel Configuration

Link to screenshot listing Admins:

Link to screenshot of personnel with Write permissions:

Cloud.gov Pages Permissions

Provide Site Manager access details for the Cloud.gov Pages platform per the Template instructions.

Site managers:

2.7 Site Vulnerability Scanning

The GSA Pages ISSO will document the following elements in the template:

Scan URL: Public URL

Scan Tool: Invicti

Scan Completed: Complete **Date:** Sep 20, 2023

PublicURL_Scan_Report: _____

PreviewURL_Scan_Report: _____

Web Application Scan

Scan Totals	Risk Levels			
	Critical	High	Moderate	Low
Original Total				
Current Total				

Application Web Scan Summary Table:

No.	Vulnerability Description	Initial Risk	Adjusted Risk (if any)	Recommended Fix	Status (Open Or Closed or False Positive)

2.8 Binding Operational Directive (BOD) 18-01 Checks

A binding operational directive is a compulsory direction to federal, executive branch, departments and agencies for purposes of safeguarding federal information and information systems. Department of Homeland Security (DHS) BOD 18-01 requires specific email and web configuration settings. Additional details about the requirements are in the Template and in BOD 18-01. The required settings will be verified by the GSA Pages ISSO once the public URL has been assigned and set up.

2.9 Approval Process

The ISSO and Site Owner collaborate to complete the GSA Pages 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. Sites will not be approved if they have any Critical or High security findings.

By signing the completed Template, the GSA Website Manager agrees to follow the GSA Pages system wide Incident Response and Configuration Management plans.

3 Maintaining Approved Sites

Sites hosted on GSA Pages are required to have their URLs scanned in accordance with CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk and GSA's parameter for National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, control RA-5, Vulnerability Scanning.

4 Reassessment

A Site's ATU will have to be reassessed and an ATU reissued if the Site is found NOT to be

in conformity with the requirements within this guide. Conditions/events that may require a reassessment and ATU reissuance include:

1. New third party integrations not on the approved list are added.
2. The data types or information presented on the site changes.
3. A significant security incident occurs.
4. There are deviations from the ATU maintenance requirements.

5 Failure to Maintain Site - Site Removal

Sites that fail to maintain the ATU requirements will be issued a formal notice. The GSA Pages team may take steps to disable the site or remediate the vulnerabilities. ATU site owners who hit certain triggers of overdue POA&Ms and/or failure to maintain alignment to ATU requirements will be required to provide a Corrective Action Plan (CAP) addressing the plan to address the deficiencies. The CAP must be approved by the Site owner, System Owner, ISSM, and IST Director. Sites or Site owners who fail to respond to a CAP, or complete approved actions will be removed from the ATO boundary and will no longer be authorized. The removal process steps are further described below:

1. Detailed Finding Review (DFR) - Site owners will be issued a DFR upon failing to address a deficiency within the site or alignment with the ATU requirements.
2. Corrective Action Plan
    a. Site Owners who fail to adequately respond or address a DFR, will be issued a CAP request.
    b. The Site Owner must provide a CAP to the System owner within 30 days of the CAP request. The CAP must detail how the team will address the deficiencies and the timeline for completion.
    c. The Site Owners CAP must be approved by the GSA Pages system owner, the ISSM, and IST Director.
3. Site Disablement
    a. Site Owners who fail to respond to the CAP within the 30 day timeframe, or fail to provide an adequate CAP, or fail to comply with the provisions, timeline and duration of their CAP will have their site Disabled.
    b. Disabling a site consists of unpublishing the site within the Cloud.gov Pages Platform which will result in a site being unreachable.
4. Site Removal
    a. Site Owners who fail to address deficiencies within 90 days of disablement will have their site removed from the GSA Pages ATO boundary and the site will be deleted.
    b. Deleting a site removes the published site from GSA Pages servers and from the dashboards of all site users. This will bring the entire site offline and make it inaccessible for users.
    c. A Site Removal letter will be issued indicating that the site is no longer authorized to operate.