



**IT Security Procedural Guide:
Robotic Process Automation (RPA)
Security
CIO-IT Security-19-97**

Revision 3


February 14, 2023

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
Initial Release – March 27, 2019				
N/A	ISE	Initial Release	N/A	N/A
Revision 1 – November 14, 2019				
1	Smith, Klemens, Dean	Requirements added for SSP updates for systems interacted with by BOTs. Updated templates and converted to Microsoft products for posting to InSite.	Reflect updated GSA guidance on documenting and approving BOTs.	Multiple
Revision 2 - March 30, 2020				
1	Nawrocki	Revised and restructured document: <ul style="list-style-type: none"> Added use of Unattended Bots within the Enterprise RPA Platform Added Orchestrator Admins role Updated authentication methods Process divided into Simple and Complex Bot processes Deleted requirement for System Owner approval and SSP updates for Simple Bot Process. 	Reflect updated risk considerations, process changes, and the use of unattended Bots.	All
Revision 3 - February 14, 2023				
1	Tydings/ Zheng/Smith	Revised and restructured document: <ul style="list-style-type: none"> Added API Questionnaire requirement. Edited and revised content. Included information based on current security requirements. Performed overall review. 	Updated to reflect current GSA process and guidance.	Throughout
2	McCormick/ Klemens	<ul style="list-style-type: none"> Clarified documentation requirements to align to current practices RPA approval process. Edited and formatted guide. Updated to align with NIST 800-53, Revision 5. 	Aligned guide to current GSA guide formatting and style.	Throughout

Approval

IT Security Procedural Guide: Robotic Process Automation (RPA) Security, Revision 3, is hereby approved for distribution.

DocuSigned by:

FD717926161544F...

Bo Berlas
GSA Chief Information Security Officer

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

Table of Contents

1	Introduction	1
1.1	Purpose	1
1.2	Scope	1
2	RPA Terminology	2
3	RPA Platforms	3
3.1	Enterprise RPA Platform (ERPA)	3
3.2	Empower IT Platform (EIP)	3
3.3	ERPA/EIP RPA Bot Approval Process Flow	3
4	Roles and Responsibilities	4
4.1	Authorizing Official (AO)	4
4.2	System Owner	4
4.3	Process Owner	5
4.4	Bot Custodian (Attended Bots Only)	5
4.5	Project Team (Development Team)	5
4.6	Bot Developer	5
4.7	Project Owner	5
4.8	RPA Information Systems Security Officer (ISSO)	6
4.9	RPA Information Systems Security Manager (ISSM)	6
4.10	RPA Platform Administrator	6
4.11	Chief Privacy Officer (CPO)	6
5	General RPA Security	6
5.1	RPA Authorizations/Access Approvals	6
5.1.1	Access Management	6
5.2	Secure Credentials Storage	7
5.3	RPA Clients Approval in IT Standards Profile	8
6	GSA RPA Methodology	8
6.1	Development of Robotic Process Automation (RPA) Clients	8
6.1.1	Development of the RPA Bot in a Test Environment	8
6.2	Approval Process for the Robotic Process Automation (RPA) Clients	9
6.2.1	Completion of Privacy Threshold Assessment	9
6.2.2	Completion of Privacy Impact Assessment	9
6.2.3	Completion of RPA Attributes Questionnaire	9
6.2.4	Simple Bot Review Process	10
6.2.5	Complex Bot Review Process	11
	Appendix A. Updating SSPPs Regarding Bot Interaction (Suggested Actions)	13

Figures and Tables

Table 2-1.	RPA Key Terms	2
Figure 3-1.	RPA Bot ATO Process	4

1 Introduction

This procedural guide provides an overview of the process by which Robotic Process Automation (RPA) Bots obtain an approval to operate in the production environment under the General Services Administration (GSA) RPA Approval to Use (ATU) process. The RPA ATU process leverages the inherent flexibility in the application of security and privacy controls noted in [National Institute of Standards and Technology \(NIST\) Special Publication \(SP\) 800-53, Revision 5](#), “Security and Privacy Controls for Information Systems and Organizations,” and [NIST SP 800-37, Revision 2](#), “Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.”

RPA Bots are used to automate repetitive tasks, which saves the organization time and money. RPA yields products with predictable results (e.g., spreadsheets, emails, forms, documents) and enables GSA to quickly and efficiently build applications to modernize its IT portfolio while promoting innovative solutions throughout the GSA Enterprise.

RPA Bots are viewed as regular users on GSA’s network and in the applications they are granted access to. GSA currently limits the use of Artificial Intelligence (AI) and/or Machine Learning (ML) in RPA to approval by exception. If an RPA Program requires the use of AI/ML, additional approval from the RPA ISSM and GSA CISO is required. Additionally, using AI/ML may require updates to: 1) the System Security and Privacy Plan (SSPP) for the system running AI/ML Bots, 2) the security controls surrounding this functionality, and 3) any relevant templates. GSA attended RPA Bots run within the Virtual Desktop Infrastructure (VDI) environment, and Unattended Bots run within the Enterprise RPA Platform (ERPA) or the EmpowerIT Platform (EIP). Bots are not permitted to run on user workstations.

1.1 Purpose

The purpose of this procedural guide is to assist GSA Federal employees and contractors with their IT security and privacy responsibilities when implementing a secure RPA process. This guide outlines the key activities for implementing the RPA Approval to Use (ATU) process.

This guide also provides instructions on obtaining an ATU for a new process being automated through the implementation of RPA, ensuring the same process is followed for each new RPA Bot.

1.2 Scope

GSA authorizes the use of Attended Bots, which run in VDI, and Unattended Bots, which run in the ERPA or EIP in accordance with the process identified in [Section 6.2](#). This guide describes the process to obtain a security ATU for RPA Bots within GSA and applies to all GSA offices in which RPA software is used to develop and/or use automations.

2 RPA Terminology

Key terms used in reference to RPA at GSA are defined in Table 2-1.

Table 2-1. RPA Key Terms

Process	Acronym	Description
Robotic Process Automation	RPA	The use of software scripts to perform tasks as an automated process, which no longer requires the use of human input.
Application Programming Interface	API	A software intermediary enabling two applications to talk to each other.
Artificial Intelligence	AI	Intelligence demonstrated by machines as opposed to humans. Note: AI Bots are limited and approved only by exception on GSA networks. An AI Bot must have explicit approval from the RPA ISSM and GSA CISO.
Attended RPA	N/A	Attended RPAs speed up repetitive front office tasks. They mimic a user's activities but require human intervention. They reside on a VDI workstation and are collaborators in service desk, helpdesk, and call center activities. They work discreetly in the background while users continue with uninterrupted work, ensuring high productivity and low handling times.
Bot	N/A	The automated version of the process that gets executed, also known as the script or code.
Enterprise RPA Platform	ERPA	The RPA Platform managed by GSA Corporate IT Services, using the UiPath suite of products.
Empower IT	EIP	The RPA Platform managed by Digital Infrastructure Technologies (DIGIT), using the Empower IT (previously NCI) suite of products.
Non Person Entity	NPE	An Active Directory (AD) user account assigned to a Robot Worker (Bot).
Machine Learning	ML	A method of data analysis that automates analytical model building. ML is a branch of artificial intelligence based on the idea that systems can learn from data, identify patterns, and make decisions with minimal human intervention. Note: ML Bots are limited on GSA networks and approved only by exception with additional approval required.
Process	N/A	Work broken into steps and turned into a script that becomes automated.
Robot Worker	N/A	Another term for Bot.
Unattended RPA	N/A	RPAs that operate without human touch, maximizing cost and performance benefits for any variety of back-office activities. They automatically complete back-office functions at scale without human intervention.

3 RPA Platforms

3.1 Enterprise RPA Platform (ERPA)

ERPA is an RPA Platform operated and managed by GSA Corporate IT Services (IC). ERPA uses UiPath Studio for the creation of Bots and UiPath Orchestrator for the administration, scheduling, and execution of Bots created by the Office of the Chief Financial Officer (OCFO).

3.2 Empower IT Platform (EIP)

EIP is an RPA platform operated and managed by the GSA Office of Digital Infrastructure Technologies (IDT). EIP is used for the creation of Bots and the Maestro application is used for the administration and execution of Bots.

3.3 ERPA/EIP RPA Bot Approval Process Flow

The RPA Bot approval process consists of:

1. Completing a Privacy Threshold Assessment (PTA) for the GSA Privacy Office to determine if a Privacy Impact Assessment (PIA) is required and completing that PIA. PTAs and PIAs are completed in GSA's Archer GRC solution (contact archersupport@gsa.gov if assistance is needed).
2. Completing an [RPA Attributes Questionnaire](#) and following the complexity process in the questionnaire.
3. Determining if an API is involved with the Bot process and including the API information in a Process Design Document (PDD) or completing the API Security Questionnaire (available on the [GSA IT Security Forms and Aids page](#)).
Note: The PDD is an RPA Team internal document. Contact rpaoffice@gsa.gov to receive the current PDD template.
4. Providing the information from the previous steps, along with all other required information described in Section 6.2 and providing the entire package to the RPA Information Systems Security Officer (ISSO) for security review.

After the security review is completed and any issues addressed, an ATU is granted by the Information Systems Security Manager (ISSM) for complex Bots or by the RPA ISSO for Simple Bots.

Figure 3-1 illustrates the RPA Bot ATU Process.

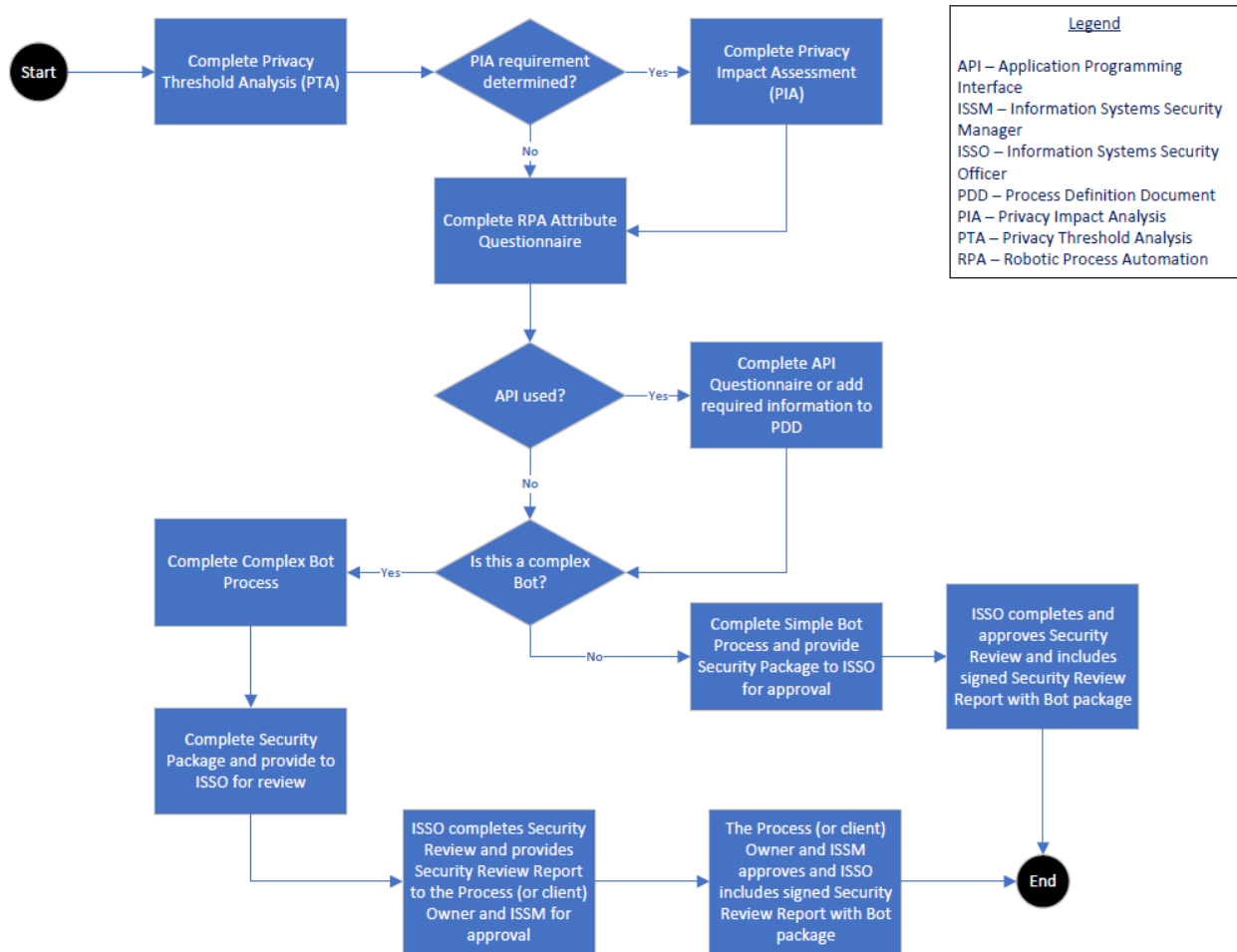


Figure 3-1. RPA Bot ATU Process

4 Roles and Responsibilities

4.1 Authorizing Official (AO)

AOs have the overall responsibility of accepting security risk and approving the Authorization to Operate for the RPA Program platforms.

4.2 System Owner

System Owners approve access for RPA Bots to their systems for the purposes defined in the GSA RPA Security Package. System Owners are also responsible for verifying that the System Security and Privacy Plans (SSPPs) for their systems are updated as described in [Section 6.2.5.6](#) and [Appendix A](#). RPA ISSOs, RPA ISSMs, etc. do not update the security documentation for the systems being accessed.

4.3 Process Owner

Process Owners are responsible for the RPA Bot on the business side. Responsibilities include the following:

- Defining the business purpose for the automation.
- Approving a PDD outlining the process to be automated using RPA.
- Liaising with the Project Team, the Bot Custodian, the System Owners of the system(s) the RPA will access, and the RPA Development Team

4.4 Bot Custodian (Attended Bots Only)

The Bot Custodian is responsible for executing attended RPA Bots, providing the credential used to execute the process, and interfacing with the Security Team to sign the GSA [RPA Bot Custodian Rules of Behavior \(ROB\)](#).

4.5 Project Team (Development Team)

The Project Team is the in-house team, business group, or contractor(s) engaged to code the process, enabling the RPA software to run the manual processes. The Project Team collaborates with the Process Owner on the process and the PDD (if the PDD exists or, if not, develops the PDD), creates a video of the automated process, and prepares a description of the actions being taken on behalf of the Bot Custodian/Process Owner. Responsibilities include:

- Completing the RPA Attributes Questionnaire required for the security review.
- Completing the API Security Questionnaire to ensure APIs listed in the RPA Attributes Questionnaire and documented in the PDD are properly accounted for in terms of security.
- Providing a copy of the API Security Questionnaire and PDD to the ISSO of the Federal Information Security Modernization Act (FISMA) system being accessed. If all of the API information required by the API Security Questionnaire is included in the PDD, then inclusion of the questionnaire is not required.
- Developing a PDD outlining the process to be automated using RPA.

4.6 Bot Developer

The Bot Developer is the in-house person, group, or contractor engaged to code the process, enabling the RPA software to run the manual process.

4.7 Project Owner

The Project Owner is accountable for the process automation and oversees the Project Team. The Project Owner approves the PDD that outlines the process that will be automated using RPA.

4.8 RPA Information Systems Security Officer (ISSO)

The RPA ISSO is the focal point in getting the RPA process authorized. The RPA ISSO works with the Project Team and the Process Developer to ensure the RPA Attributes Questionnaire is complete and accurate. The RPA ISSO also works with the Project Team and the Privacy Office to complete the PTA and PIA if required. Once complete, the RPA ISSO collects and saves all artifacts in a central location within a Google shared drive. The ISSO reviews and approves Simple Bots for use, and, for Complex Bots, reviews and forwards the package to the ISSM for final review and approval.

4.9 RPA Information Systems Security Manager (ISSM)

The RPA ISSM is the final approval authority of Complex Bots to be included in the GSA RPA ATU package. The RPA ISSM reviews the RPA Attributes Questionnaire and artifacts after they have been compiled by the RPA ISSO and relays their concurrence that the security measures have been met and that the RPA is approved for use in accordance with this guide.

4.10 RPA Platform Administrator

System administrators for the Unattended Platform (UiPath Orchestrator for ERPA or Maestro for EIP) oversee the information system that the Unattended Bots run on. They assist the Project Team in the troubleshooting of Bots and other performance and execution issues.

4.11 Chief Privacy Officer (CPO)

GSA's Privacy Officer is the final approval authority for the PTA and PIA (if required) to be included in the RPA ATO package. GSA's CPO signs all final documentation.

5 General RPA Security

The following sections describe general processes and requirements that must be applied to all RPA Bots in use at GSA.

5.1 RPA Authorizations/Access Approvals

The Project Team must use GSA-defined rules of behavior (see [Section 4.4](#)) and ensure [RPA System Access Approval Forms](#) are completed for Complex Bots.

5.1.1 Access Management

Attended Bots use the credentials of the Bot Custodian stored in the secure Credential Manager (Windows Security Credentials Password Vault) of the underlying Windows Operating System (OS). Credentials are stored on the hard drive and protected by using the Data Protection Application Programming Interface (DPAPI). Any program running as that user can access credentials in this store. Credential Manager uses the Credential Locker, formerly known as Windows Vault, for secure storage of usernames and passwords.

Unattended Bots use a distinct Active Directory (AD) account, known as a Non-Person Entity (NPE), with credentials managed by CyberArk to ensure frequent password rotation. Least privilege is followed when assigning access permissions to the Bot. In cases where multiple automations require the same access permissions, multiple automations may use the same NPE. Automations requiring elevated permissions (i.e., permissions greater than a standard user) must use a separate NPE. NPE accounts with elevated privileges are limited to one NPE account per process unless explicitly approved by the RPA ISSM.

There are three different authentication configurations under RPA:

1. Attended Bots using the GSA enterprise authentication service (SecureAuth for single sign on);
2. Attended Bots using basic authentication or Windows Integrated Authentication; and
3. Unattended Bots using NPE accounts.

Each configuration is described below.

Attended Bots using GSA enterprise authentication service. To authenticate Attended Bots, the enterprise authentication service (SecureAuth for single sign on (SSO)) capabilities are utilized so the Attended Bots run under a specific user's account. If SSO is enabled, a user can access the application(s), then the attended Bot is able to access the application on behalf of the user.

Attended Bots using Windows Integrated Authentication or basic authentication. When local applications are involved in the automation process, Windows Integrated Authentication, or basic authentication (using username and password) may be used in accordance with existing policies governing their use.

Unattended Bots using NPE accounts. For Unattended Bots, CyberArk manages the Robot User credential and provides support for UiPath Orchestrator and Maestro.

For Bots using APIs, API authentication requirements are addressed in [CIO-IT Security-19-93: Application Programming Interface \(API\) Security](#).

5.2 Secure Credentials Storage

For Attended Bots, if credentials are stored in the RPA Bot, it must be ensured they cannot be accessed without appropriate authentication. All sets of generic credentials stored in Credentials Manager for the current user must be accessible only to the current user's processes and must not be shared with or accessible to the other OS users, not even in a multi-user OS. For Attended Bots that must store credentials locally on a Windows machine, the credentials must be stored in the Windows Credential Store or as an "Asset" within Orchestrator and invoked by the workflow/robot only.

For Unattended Bots, CyberArk Bot software is used on the Orchestrator and ERPA Robot servers, as well as on EmpowerIT servers, to securely store Robot User credentials.

5.3 RPA Clients Approval in IT Standards Profile

RPA Bots must be developed using software approved in GSA's official [IT Standards Profile](#), which contains a list of all software technologies and applications acquired and approved for use at GSA. The security review of any new RPA Bot applications shall ensure encryption meets GSA standards.

6 GSA RPA Methodology

6.1 Development of Robotic Process Automation (RPA) Clients

This section describes the process for developing, testing, obtaining approval to deploy, deploying, and operating RPA Bots at GSA.

Note: The ERPA and EIP are platforms governed by the GSA Enterprise Change Control Board. Major changes to the platform are defined and controlled by GSA Change Management Policies.

Any modification to an Attended or Unattended Bot that changes the approved security posture of the Bot will require an updated Bot submission for review by the security team. Bots are managed by submitting the updated Bot package through the relevant approval process. However, the submission package should specify all changes made to the Bot to support a more accurate and proficient security review by the RPA ISSO and RPA ISSM. Any new connections made to new information systems (requiring System Owner approval and SSPP updates) are not considered changes in the context of Bot Change Control; instead, new or modified system connections for an existing Bot package require re-submission and re-approval of the PDD and associated ATO documents prior to use.

6.1.1 Development of the RPA Bot in a Test Environment

To begin development, members of the business lines meet with the RPA developer to review the PDD and requirements of the RPA Bot. Then, the developer prepares the automated process for testing in the VDI, ERPA, or EIP Test Environment. Websites that the RPA Bot needs to access in ERPA or EIP, are granted by filling out an [RPA Whitelisting Request](#).

A member of the Project Team makes a video recording of the automation with voice over describing the actions being automated and conducts a workflow extraction. The video and workflow extraction are shared with the RPA ISSO and Privacy Office and must be included in the RPA Security Package. At the same time, the Project Team coordinates with the Process Owner to begin user acceptance testing (UAT). UAT and the security approval process can run in parallel.

6.2 Approval Process for the Robotic Process Automation (RPA) Clients

The requirements to obtain approval for the RPA Bots are outlined in the following sections. Any changes that impact the approved security posture of a Bot will require a new security review.

The approval process is dependent on results for calculated complexity as assessed in the RPA Attributes Questionnaire. Only Bots determined to be Complex Bots require the full workflow.

Note: Bots previously approved under the original version of this guide (dated 11-14-2019) inherit approval sufficient for Complex Bots. However, the original request along with the new RPA Attributes Questionnaire must be submitted to migrate an Attended Bot to the ERPA.

6.2.1 Completion of Privacy Threshold Assessment

All Bot approvals start with the PTA which identifies if any personally identifiable information (PII) is involved in the process being automated. The PTA information is populated and processed in GSA's Archer GRC solution by the RPA Process Owner and Custodian. All API use must be documented in the PTA. The RPA ISSOs and the Privacy Office are notified upon completion to allow for review and approval of the PTA. Notes in the PTA will indicate whether the Privacy Office requires a PIA as well.

6.2.2 Completion of Privacy Impact Assessment

The business line and the Project Team are responsible for creating and completing any PIA/PTA documentation required to support the Bot package(s). If a PIA is needed, it goes against the system containing sensitive information that the automation is interacting with. The PIA is not done for the Bot package or the boundary that contains the Bot itself. PIAs are populated and processed in GSA's Archer GRC solution. Additional information on PTAs/PIAs is available on the GSA [Privacy](#) page. GSA's [Privacy Impact Assessments \(PIA\)](#) page provides information to assess applicability of any existing PIAs. The RPA ISSOs and the Privacy Office are notified upon completion of the PIA to allow for review and approval. The final PIA is then posted on GSA's website for the public to view.

6.2.3 Completion of RPA Attributes Questionnaire

The RPA Project Team works to complete the RPA Attributes Questionnaire. Once complete, the questionnaire is used to determine if the Bot is Complex or Simple. This determination is performed alongside the RPA ISSO. If any concerns are raised by the FISMA system ISSO or RPA ISSO, they are addressed before moving forward. At this time, the RPA ISSO also reviews the video recording and workflow extraction provided by the RPA Project Team and any concerns must be addressed.

Depending upon the calculated complexity determined through the RPA Attributes Questionnaire, the RPA Project Team follows either the Simple or Complex Bot review processes described in the following sections.

6.2.4 Simple Bot Review Process

Simple Bots are determined by answering the risk qualification questions on the Calculations tab in the RPA Attributes questionnaire. If it is determined all were answered “No,” then the Bot is considered “Simple.” If any questions were answered “Yes,” then the Bot is considered “Complex.”

Simple Bots require only ISSO approval. Complex Bots must be approved by the ISSO and ISSM (skip to [Section 6.2.5](#) for Complex Bot procedures).

Refer to the “Simple” tab of the RPA Attributes Questionnaire and provide the required information for all steps.

6.2.4.1 Submit Package for Review to RPA ISSO

The Project Team compiles the RPA package and provides it to the RPA ISSO. The RPA package includes, but is not limited to:

- RPA System Access Approval form
- Recording of the RPA
- RPA Attributes Questionnaire
- API Questionnaire, if applicable
- PDD
- PTA/PIA
- Workflow extraction
- Screenshots (In the PDD)
- Data flow diagrams (In the PDD)

The RPA System Access Approval form and the RPA Attributes Questionnaire can be found on the [GSA IT Security Forms and Aids page](#).

6.2.4.2 ISSO RPA Review

The RPA ISSO reviews all artifacts, ensuring all documentation refers to the associated RPA, and then determines the Bot’s suitability for acceptance into production. Upon receipt of the package, the RPA ISSO enters the Bot into the GSA RPA Security tracking inventory and records the necessary information. If all information is presented and complete, the Bot may be promoted to production and used according to the Rules of Behavior, the change process described in [Section 6.1](#) and the Bot Annual Review described in [Section 6.2.4.4](#).

6.2.4.3 Simple Bot Promotion

After review and with RPA ISSO approval, the Bot is promoted from testing to production and begins operation. The RPA ISSO notifies the RPA Project Team, and then the RPA Project Team notifies the Process Owner to let them know that production use of the Bot is approved.

6.2.4.4 Bot Annual Review

The individually approved RPA Security Package becomes part of a larger, singular RPA Platform ATO. All individual RPA Security Packages expire when the GSA RPA Platform ATO expires. Each package requires a review to become operable with the issuance of the new GSA RPA Platform ATO. The RPA Bot Package PTA must be reviewed and updated annually.

6.2.5 Complex Bot Review Process

Complex Bots must be approved by the ISSO and ISSM. Refer to the “Complex” tab of the RPA Attributes Questionnaire and provide the required information for all steps.

6.2.5.1 Obtain GSA System Owner Approval

Approval from the System Owner, ISSO, and ISSM of all information systems the RPA Bot will access is required. This ensures the System Owners throughout the Enterprise are aware and agree to authorize RPA Bot access using the RPA System Access Approval Form. After approval of the Form, the System Owner/ISSM may decide that an update to the system SSPP is required and add the additional information they deem necessary.

6.2.5.2 Submit Package for Review

The Project Team compiles the RPA package and provides it to the RPA ISSO. The RPA package is described in [Section 6.2.4.1](#).

6.2.5.3 ISSO RPA Review

The RPA ISSO reviews all artifacts, ensuring all documentation refers to the associated RPA, and determines the Bot’s suitability for promotion to production. Upon receipt of the package, the RPA ISSO enters the Bot into the RPA tracking inventory and records the necessary information. The Bot package includes acknowledgement from the affected System Owners and/or FISMA System ISSOs. If the Bot runs with a Robot User NPE, the recording and workflow extraction are used to validate and correct the specific access permissions required for the Bot to perform its functions. If all information is presented and complete, the RPA ISSO forwards the package to the RPA ISSM for review and approval. Once the Bot is complete and the RPA ISSM has approved its usage, the Approval Date column in the Bot Inventory Tracking Sheet is updated with the package signature date.

6.2.5.4 ISSM RPA Review and Bot Promotion

Once all security documentation (including the PTA and PIA, if required) is completed and reviewed by the RPA ISSO, the RPA Security Package is sent to the ISSM for final review determination for suitability to production. If approved, the RPA ISSO notifies the Process Owner and Orchestrator Administrator that the Bot is approved and authorized for use in the production environment according to the Rules of Behavior, the change process described in Section 6.1 and the Bot Annual Review described in [Section 6.2.5.6](#).

6.2.5.5 Baseline Attributes

For Unattended Bots using NPEs, the Bot Developer develops basic baseline attributes describing the expected behavior of the Bot where possible and practical. These include but are not limited to:

- Name of NPE user
- Expected run time
- Expected run frequency
- Average of file access reads and writes
- Maximum data publication potential.

6.2.5.6 Bot Annual Review

This individually approved RPA Security Package becomes part of a larger RPA Platform ATO. All individual RPA Security Packages expire when the RPA Platform ATO expires, and each requires a review to become operable with the issuance of the new RPA Platform ATO. The RPA Project Team must ensure that the Bot package PTA/PIAs are reviewed annually, and any changes that could impact the privacy and security aspects of the Bot are reviewed and processed accordingly.

Appendix A. Updating SSPPs Regarding Bot Interaction (Suggested Actions)

When a Bot is interacting with a FISMA system, the FISMA System Owner and the system ISSM should review the following sections of the SSPPs and make any updates they deem necessary.

1. Update the SSPP to add the interaction with Bots as part of the System Description in **Section 9, General System Description**. This section must include a listing of all Bots that interact with the system and a reference/link to the RPA(s) for the listed Bots.
2. **Section 10.4, Data Flow (and Figure 10-1)**. Include the data flows associated with Bots. Note that the PDD for Bots must include Process Flows and detailed process steps. The PDD can be referenced within Section 10.4 and attached as a supporting document, or the Bot Data Flow can be added.
3. **Section 10.6, Ports, Protocols, and Services (and Table 10-4)**. should include ports/protocols/services used by Bots, if any, and include Bot use in the purpose column. If an existing port, protocol, or service is used, add Bot use in the purpose statement.
4. **NIST SP 800-53 Security Controls**. The following security controls are to include information about Bots, when Bot-specific actions, attribution, or interaction can be ascertained.

NOTE: Under current NIST and GSA guidance, the controls listed below are only applicable at the Federal Information Processing Standards Publication (FIPS) Pub 199, “Standards for Security Categorization of Federal Information and Information Systems” levels indicated within the FIPS Levels column (L-Low, M-Moderate, H-High).

In the cases of a Bot interacting with a FIPS Low system where the control is not applicable, the affected Low system is required to include the control, but only as it pertains to the Bot.

Table A-1. Recommendations for NIST Control Implementation Regarding BOTs

NIST Control	FIPS Levels	Instructions for Control Implementation
AC-2: Account Management	L, M, H	Revise to include the usage of Bots. If Bot accounts Bots are managed differently than other accounts, explain the difference.
AC-6: Least Privilege	M, H	Revise to include the usage of Bots. If any Bot privileges are different from the custodian running the Bot, describe how privileges are handled.
AC-6(2): Least Privilege Non-Privileged Access for Nonsecurity Functions	M, H	Revise to include the usage of Bots. If any Bot privileges are different from the custodian running the Bot, describe how privileges are handled.
AC-6(5): Least Privilege Privileged Accounts	M, H	Revise to include the usage of Bots. If any Bot privileges are different from the custodian

NIST Control	FIPS Levels	Instructions for Control Implementation
		running the Bot, describe how privileges are handled.
AC-6(10): Least Privilege Prohibit Non-Privileged Users from Executing Privileged Functions	M, H	Revise to include the usage of Bots. If any Bot privileges are different than the custodian running the Bot, describe how privileges are handled.
IA-2: Identification and Authentication (Organizational Users)	L, M, H	Revise, to include the usage of Bots. Describe if Bots use their own or custodian's identifiers and authenticators or a named Robot User.
IA-2(1): Identification and Authentication (Organizational Users) Multi-Factor Authentication to Privileged Accounts	L, M, H	Revise, to include the usage of Bots. Describe if Bots use their own or custodian's identifiers and authenticators or a named Robot User. Describe how MFA is implemented.
IA-2(2): Identification and Authentication (Organizational Users) Multi-Factor Authentication to Non-Privileged Accounts	L, M, H	If Bots have or use non-privileged accounts, describe how MFA is supported.
IA-5: Authenticator Management Manage system authenticators by: (c) Ensuring that authenticators have sufficient strength of mechanism for their intended use; (f) Changing or refreshing authenticators [one time use passwords must expire in two minutes if based on a real-time clock] or when [compromised, recovered/forgotten, or due to incident related events] occur; (g) Protecting authenticator content from unauthorized disclosure and modification; (i) Changing authenticators for group or role accounts when membership to those accounts change.	L, M, H	Describe how the authenticators used by Bots (their own or Custodians') are managed, especially regarding the conditions under which they are changed.
PL-4: Rules of Behavior	L, M, H	In the control implementation discussion, include a reference and link to the Bot Custodian Rules of Behavior for any Bots interacting with the system.
SC-8: Transmission Confidentiality and Integrity	M, H	Update to identify whether Bots are using existing transmission means or whether additional transmission means have been established for Bots. Ensure web services connections are secured.
SC-8(1): Transmission Confidentiality and Integrity Cryptographic Protection	M, H	Update to identify whether Bots are using existing transmission means or whether additional transmission means have been established for Bots. Ensure web services connections are secured.