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

Revision 2

March 31, 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 – March 27, 2019		
N/A	ISE	Initial Release	N/A	N/A
		Revision 1 – November 14, 2019		
Revision 1 – March 31, 202019				
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 31, 2020		
1	Nawrocki	Revised and restructured document: • 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 the Simple Bot Process • Clarified responsibilities for tracking RPA approvals and maintaining inventory sheet	Reflect updated risk considerations, process changes, and the use of unattended Bots.	All

Approval

IT Security Procedural Guide: Robotic Process Automation (RPA) Security, CIO-IT Security 19-97, Revision 2, 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

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 Authorization to Operate (ATO). The RPA ATO process leverages the inherent flexibility in the application of security controls noted in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, "*Security and Privacy Controls for Federal 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 complete tasks that are repetitive in nature, freeing up time for personnel to perform work that truly requires human input. RPA yields products with predictable results, such as spreadsheets, emails, forms and documents. In doing so, RPA enables GSA to quickly and efficiently build applications to modernize its IT portfolio while promoting innovative solutions throughout the GSA Enterprise.

RPA Bots on GSA's network are viewed as regular users on the network and in the applications, they are granted access to. The use of RPA in GSA does not include any type of Artificial Intelligence (AI) and thus is not capable of learning or creating efficiencies by itself. Attended RPA Bots in GSA run within the Virtual Desktop Infrastructure (VDI) environment, and Unattended Bots run within the Enterprise RPA Platform (EPRA). No Bots are permitted to run on any user workstations.

1.1 Purpose

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

In addition, this procedural guide will provide instructions on how to obtain approval to operate for a new process that is being automated through the implementation of RPA and to ensure the same process is followed for each new RPA Bot.

1.2 Scope

GSA authorizes the use of unattended and attended Bots (i.e., RPA Bots) in VDI and EPRA in accordance with the process identified in Section 5.2. The scope of this guide is to provide the process to obtain approval for the RPA Bots.

2 RPA Terminology

Key terms used in reference to RPA at GSA are defined as follows:

RPA: The use of software scripts to perform tasks as an automated process that no longer requires the use of human input.

Process: A process is work that is broken into steps and then turned into a script that becomes automated.

Bot: The automated version of the process that gets executed, also known as the script or code.

Robot Worker: Another term for Bot.

Attended RPA: An attended RPA, through code, speeds up repetitive front office tasks. They mimic a user's activities; but require human intervention. They reside on a VDI workstation and are perfect collaborators in service desk, helpdesk, and call center activities. They work discreetly in the background while the users continue with uninterrupted work, ensuring high productivity, and low handling times.

Unattended RPA: Unattended RPAs operate without human touch, maximizing cost and performance benefits for any variety of back-office activities. RPAs automatically complete back-office functions at scale without human intervention.

3 Roles and Responsibilities

3.1 Authorizing Officials (AOs)

AOs have the overall responsibility of accepting risk and approving the authorization to operate for the RPA Program.

3.2 System Owners (SOs)

SOs approve access for RPA Bots to their systems for the purposes defined in the GSA RPA Security Package. SOs are also responsible for verifying the SSPs for their systems are updated as described in Section 5.2.4 and Appendix A.

3.3 Process (Bot) Owners

Process Owners are responsible for the RPA Bot on the business side. The Process Owner has multiple responsibilities:

- Drafting a Process Design Document (PDD) outlining the process to be automated using RPA.
- Liaising with the RPA Developer, the RPA Custodian, the System Owners of the systems the RPA will access, and the Privacy Office and Security Team.
- Completing the RPA Attributes Questionnaire required for the security review. The questionnaire is available on the IT Security Forms and Aids page.

3.4 Bot Custodians (Attended Bots Only)

The Bot Custodian is the person responsible for executing attended RPA Bots and providing the credential used to execute the Process; and for interfacing with the Security team to sign the

GSA Robotic Process Automation Bot Custodian Rules of Behavior. The RPA Bot Custodian Rules of Behavior is available on the IT Security Forms and Aids page.

3.5 Process Developers

The Process Developer is the in-house person, group, or contractor engaged to code the process, allowing for the manual process to be run by the RPA software. As part of the process the developer collaborates with the Process Owner on the PDD, and develops a video of the process, as well as a description of the actions being taken on behalf of the Bot Custodian.

3.6 Information Systems Security Officer (ISSO)

The ISSO is the focal point in getting RPAs through the approval process and approved. The ISSO works with the Process Owner and the Process Developer to ensure the RPA Attributes Questionnaire is complete and accurate. The ISSO also works with the Process Owner as well as the Privacy Office to complete the Privacy Threshold Assessment.

The ISSO tracks all Bots, manages the approval workflows and status, and approves Simple Bots. For Complex Bots, the ISSO reviews and forwards the package to the Information System Security Manager (ISSM) for final review and approval. The ISSO updates the RPA tracking sheet as Bots are approved.

3.7 Information Systems Security Manager (ISSM)

The ISSM is the final approval authority for Complex RPA Bots. The ISSM reviews the RPA Attributes Questionnaire and artifacts after they have been compiled by the ISSO and relays their concurrence that the security measures have been met, and that the RPA is allowed to operate in accordance with this guide.

3.8 Orchestrator Admins

System administrators for the Unattended Platform (UI Path Orchestrator) oversee the Information System that the Unattended Bots run on. They assist Bot Owners in the troubleshooting of Bots and other performance and execution issues.

3.9 Chief Privacy Officer (CPO)

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

4 General RPA Security

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

4.1 RPA Authorizations/Access Approval

The Bot Custodian must use GSA-defined rules of behavior (see Section 3.4) and ensure system access approval forms are completed for Complex Bots.

4.1.1 Authorization

For Attended Bots, the RPA 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 will be able to access credentials in this store. Credential Manager uses the Credential Locker, formerly known as Windows Vault, for secure storage of usernames and passwords.

For Unattended Bots, a distinct Active Directory (AD) account, known as a "Robot User AD account", is created that uses credentials managed by CyberArc to ensure frequent password rotation. Only the barest access permissions are assigned to the Bot. In cases where multiple automations require the same access permissions, multiple automations may use the Robot User AD account.

4.1.2 Authentication

There are three different authentication configurations under RPA: Attended Bots using SSO; Attended Bots using basic authentication or Windows Integrated Authentication; and Unattended Bots using SSO. Each is described below.

Attended Bots using SSO. In order to authenticate Attended Bots, Single Sign-on (SSO) capabilities are utilized so that the Attended RPA Bots run under a specific user's account. So, as long as SSO is enabled for a user, then SSO is also enabled for RPA.

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 SSO. For Unattended Bots, CyberArc manages the Robot User credential and provides for SSO support through UIPath Orchestrator.

4.2 RPA Bot Activity Logging

To ensure that Bot actions can be properly monitored, Bots must log all Bot activity. Attended Bots' logs must be reviewed weekly by the Bot custodians and include the capability for a complete audit trail of activities for use by GSA auditors, including data needed to identify abnormal spikes in activity, access of specific systems, and use of privileged accounts. For Unattended Bots, Orchestrator must be configured to provide for verbose logging of all robot activities. Review of Orchestrator logs is performed as part of the ERPA authorization.

4.3 Secure Credentials Storage

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

For Unattended Bots, use CyberArc Bot software on the Orchestrator and Robot servers to provide for the secure storage of Robot User credentials.

4.4 RPA Clients Approval in IT Standards Profile

RPA Bots must be developed using software approved in GSA's official IT Standards Profile. The GSA IT Standards Profile process is used to maintain a listing of all software technologies and applications that have been acquired and approved for use at GSA. The Security Review of any new RPA Bot applications shall ensure encryption meets GSA standards.

5 GSA RPA Methodology

5.1 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.

Important! The ERPA Platform is governed by the GSA Enterprise Change Control Board. Major changes to the platform are defined and controlled by GSA Change Management Policies.

All changes to Bots are managed by resubmitting the Bot through the relevant approval process; Attended or Unattended. However, the submission package should specify all the changes made to the Bot to support a faster review by the ISSO and ISSM. Any new connections made to new Information Systems (requiring System Owner approval and SSP updates) are not considered changes in the context of Bot Change Control; instead, new Information System connections require the submission and approval of a new Bot package.

5.1.1 Development of the RPA Bot in a Test Environment

To begin development, members of the business lines meet with the RPA developer to go over the PDD and requirements of the RPA Bot. Then, the developer prepares the automated process ready for testing in VDI or the ERPA Test Environment and websites that the RPA Bot needs to access in VDI or ERPA are granted by filling out the RPA Whitelisting Request Google Form.

When the business representatives determine that the RPA Bot satisfies their needs in the test environment, a member of the development team makes a video recording with voice over that

describes the actions being automated and conducts a workflow extraction. The video is shared with the ISSO and Privacy Office to begin the approval process. At the same time, the video is shared with the process owner and users to begin user acceptance testing. UAT and the approval process run in parallel. This video must be included in the RPA Security Package.

The requirements to obtain approval on the RPA Bots are outlined in the following sections. Additionally, any major changes that occur to a particular RPA Bot after already receiving an approval will require a new security review.

The process approval process is dependent on results for calculated complexity as assessed in the RPA Attributes Questionnaire available on the IT Security Forms and Aids page. Only Bots determined to be complex require the full workflow.

Note: Bots previously approved under the original RPA Process Automation Security (Revision 1, dated 11-14-2019) will inherit approval sufficient for complex Bots. However, the original request along with the new RPA Attributes Questionnaire must be submitted in the request to migrate an attended Bot to the ERPA.

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

The requirements to obtain approval on the RPA Bots are outlined in the following sections. Additionally, any major changes that occur to a particular RPA Bot after already receiving an approval will require a new security review.

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

Note: Bots previously approved under the original RPA Process Automation Security (11-14-2019) will inherit approval sufficient for complex Bots. However, the original request along with the new attributes RPA Attributes Questionnaire must be submitted in the request to migrate an attended Bot to the ERPA.

5.2.1 Completion of Privacy Threshold Assessment

All Bot approvals start with the PTA. It is used to identify any personally identifiable information (PII) involved in the process that is being automated. The PTA Google Form is completed by the RPA Process Owner and Custodian. The ISSOs are notified as well as the Privacy Office upon completion to allow for review and approval of the PTA. Please refer to Admin Notes in the PTA form to see if the Privacy Office requires a PIA as well.

5.2.2 Completion of Privacy Impact Assessment

If a PIA is required in addition to a completed PTA, the RPA Process Owner and the Business Side must complete an existing PIA may be updated or a new one should be drafted using GSA's PIA template available on the Privacy Web page. Please consult GSA's PIA inventory to assess applicability of any existing PIAs. The ISSOs are notified as well as the Privacy Office upon

completion to allow for review and approval of the PIA. The final PIA is then posted on GSA's website for the public to view.

5.2.3 Completion of RPA Attributes Questionnaire

The RPA Custodian along with the RPA Process Owner will work to complete the RPA Attributes Questionnaire. Once complete, the RPA Attributes Questionnaire is used to determine if the Bot is Complex or Simple. This determination is to be performed alongside the RPA ISSO. If any concerns are raised by the ISSO, they are addressed before moving forward. At this time, the ISSO will also review the video recording and workflow extraction that has been provided of the RPA Process Owner and likewise any concerns that arise must be addressed.

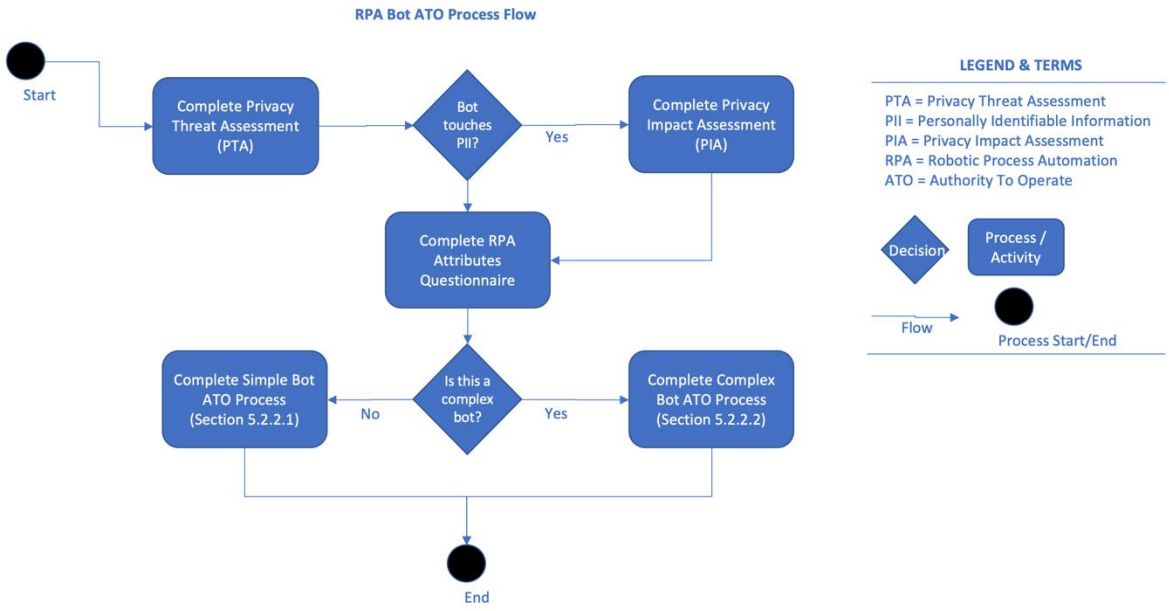

Figure 5.2.3-1. RPA Bot ATO Process Flow

Depending upon the calculated complexity determined through the RPA Attributes Questionnaire, the Bot Custodian and the Process Owner must also submit additional security documents for Complex Bots. The templates for these documents are available on the IT Security Forms and Aids page.

5.2.4 Simple Bot Review Process

Note: If your Bot is determined to be complex, skip to Section 5.2.5 of this Guide

Refer to the 'Simple' tab of the RPA Attributes Questionnaire and complete the form and provide the required information for all 11 steps.

5.2.4.1 Submit Package for Review to RPA ISSO

Prepare the recording, RPA Attributes Questionnaire, UAT results, workflow extraction, whitelisted websites, screenshots, and data flow diagrams, and provide to the RPA ISSO.

5.2.4.2 RPA ISSO review

RPA ISSO reviews all artifacts and makes a determination on 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. 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, and the Annual Review.

5.2.4.3 Bot Promotion

After review and with ISSO approval, the Bot is promoted from testing to production and begins operation. The RPA ISSO notifies the Bot Owner that production use of the Attended Bot is authorized.

5.2.4.4 Bot Annual Review

The individually approved RPA Security Package becomes part of a larger singular Enterprise wide RPA ATO. All individual RPA Security Packages will expire at once in correspondence with the expiration of the GSA RPA ATO and each will require an annual review to become operable with the issuance of the new GSA RPA ATO. The individual Bot owners must annually submit to the RPA ISSO an export of their Bot's functional process (workflow extraction.) This is then compared by the ISSO to the original approved submission to ensure that no changes have been made to the original Bot.

5.2.5 Complex Bot Review Process

Refer to the 'Complex' tab of the RPA Attributes Questionnaire and complete the form and provide the required information for all 18 steps

5.2.5.1 Obtain GSA System Owner Approval

Approval from all System Owners of all Information Systems the RPA Bot will be accessing is required. This ensures the system owners throughout the Enterprise are aware and agree to authorize this to occur using the GSA System Access Approval Robotic Process Automation form.

5.2.5.2 Update the System Security Plans

The Bot Custodian, the RPA Process Owner and ISSO must update the Systems Security Plan (SSP) for any systems that Bots interact with to identify the interaction, update affected SSP sections and update NIST controls to describe how Bots interact with the information system.

The SSP sections and a list of controls from NIST SP 800-53, Revision 4, "*Security and Privacy Controls for Federal Information Systems and Organizations"* are provided in Appendix A with

information on how they need to be updated to address Bot interaction with systems according to calculated Risk from the RPA Attributes Questionnaire.

5.2.5.3 Submit Package for review

Prepare the recording, RPA Attributes Questionnaire, UAT results, workflow extraction, whitelisted websites, screenshots, and data flow diagrams to the RPA ISSO.

5.2.5.4 RPA ISSO review

RPA ISSO reviews all artifacts and makes a determination on the Bot's suitability for promotion and authorization in Production . Upon receipt of the package, the RPA ISSO enters the Bot into the RPA tracking inventory and records the necessary information, including acknowledgement from the affected Information System (IS) System Owners and/or ISSOs. If the Bot is to be run in EPRA with a Robot User NPE, the recording and workflow extraction are used to validate and correct the very narrowly scoped access permissions required for the Bot to perform its functions. If all information is presented and complete, RPA ISSO forwards the package to the RPA ISSM for review and approval.

5.2.5.5 ISSM Reviews the RPA Security Package for Authorization

Once all security documentation (including the PTA) is completed and reviewed by the ISSO, the RPA Security Package is sent to the ISSM for final review determination for suitability to production. If approved, the RPA ISSM notifies the Bot Owner and Orchestrator Admin that the Bot is approved and authorized for use in the EPRA Production environment according to the Rules of Behavior, the Change Process, and the Annual Review.

5.2.5.6 ISSO Baseline monitoring characteristics development

For Unattended Bots using NPEs in the ERPA, the ISSO will develop basic baseline attributes that describe the expected behavior of the Bot. These include, but are not limited to: Name of NPE user, expected run time, expected run frequency, high average of file access reads and writes, maximum data publication potential, etc. These attribute profiles are provided to the GSA Security Operations Center for the development of specific monitoring triggers to alert on anomalous Unattended Bot behavior.

5.2.5.7 Bot Annual Review

This individually approved RPA Security Package becomes part of a larger singular Enterprise wide RPA ATO. All individual RPA Security Packages will expire at once in correspondence with the expiration of the GSA RPA ATO and each will require an annual review to become operable with the issuance of the new GSA RPA ATO. The individual Bot owners must annually submit to the RPA ISSO an export of their Bot's functional process (workflow extraction.) This is then compared by the ISSO to the original approved submission to ensure that no changes have been made to the original Bot.

5.2.6 Update the System Security Plans

The Bot Custodian, the RPA Process Owner and ISSO must update the Systems Security Plan (SSP) for any systems that Bots interact with to identify the interaction, update affected SSP sections and update NIST controls to describe how Bots interact with the information system.

The SSP sections and a list of controls from NIST SP 800-53, Revision 4, "*Security and Privacy Controls for Federal Information Systems and Organizations"* are provided in Appendix A with information on how they need to be updated to address Bot interaction with systems according to calculated Risk from the RPA Attributes Questionnaire.

Appendix A: Updating System Security Plans Regarding BOT Interaction

When a Complex Box is interacting with a FISMA system, the FISMA System's SSPs must be updated in the following ways:

1. Update the SSP 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 10.5, 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 10.5 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 FIPS Levels indicated within the FIPS Levels column (L, M, H).

In the cases of a Complex Bot interacting with a FIPS 199 Low system that has a given control tailored out of applicability, the affected Low system will now be required to include the control, but only as it pertains to the Bot.

Table A-1: Instructions on 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 accounts used by Bots are managed differently than other accounts on the system explain how they are managed.
AC-6: Least Privilege	M, H	Revise, to include the usage of Bots. If privileges of any Bots are different than 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 privileges of any Bots are different than 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 privileges of any Bots are different than the custodian 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 privileges of any Bots are different than the custodian running the Bot describe how privileges are handled.

NIST Control	FIPS Levels	Instructions for Control Implementation
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. If Bots have or use privileged accounts, describe how MFA is implemented.
IA-2(1): Identification And Authentication (Organizational Users) | Network Access 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. If Bots have or use privileged accounts, describe how MFA is implemented.
IA-2(2): Identification And Authentication (Organizational Users) | Network Access To Non-Privileged Accounts	M, H	If Bots have or use non - privileged accounts, describe how MFA is supported.
IA-5: Authenticator Management (c) Ensuring that authenticators have sufficient strength of mechanism for their intended use; (g) Changing/refreshing authenticators [Assignment: organization-defined time period by authenticator type]; (h) Protecting authenticator content from unauthorized disclosure and modification; (j) Changing authenticators for group/role accounts when membership to those accounts changes.	L, M, H	Describe how the authenticators used by Bots (their own or Custodians) are managed, especially with regard to the conditions under which they are changed.
PL-4: Rules of Behavior	L, M, H	A reference and link to the Bot Custodian Rules of Behavior for any Bots interacting with the system need to be included in the control implementation discussion.
SC-8: Transmission Confidentiality and Integrity	M, H	Update to identify if Bots are using existing transmission means or additional transmission means have been established for Bots. Secure web services connections are secured.
SC-8(1): Transmission Confidentiality and Integrity | Cryptographic or Alternate Physical Protection	M, H	Update to identify if Bots are using existing transmission means or additional transmission means have been established for Bots. Secure web services connections are secured.