Office of Audits
Office of Inspector General
U.S. General Services Administration

GSA Should Strengthen the Security of Its Robotic Process Automation Program

Report Number A230020/B/T/F24004
August 6, 2024

Executive Summary

GSA Should Strengthen the Security of Its Robotic Process Automation Program

Report Number A230020/B/T/F24004
August 6, 2024

Why We Performed This Audit

In 2018, the Office of Management and Budget recommended that federal agencies use robotic process automation (RPA) as a new technological tool to reduce repetitive administrative tasks.[1] That same year, GSA established its RPA program to automate low-value, routine tasks, allowing its employees to spend more time on challenging work. RPA uses bots, which are software applications that simulate human actions to reduce repetitive administrative tasks. These bots interact with existing systems to copy data, fill in forms, sign into applications, and send emails. In 2019, GSA established the Federal RPA Community of Practice, which seeks to: (1) increase RPA adoption across the federal government and (2) help agencies overcome technical, management, and operational challenges that arise in designing and deploying an RPA program.[2]

While RPA offers the potential to save time and improve productivity, the bots' ability to perform thousands of read, write, and deletion actions at high rates of speed poses unique risks to GSA's systems and data. This can make it difficult to identify logic and processing errors—and their associated consequences—before serious damage is done. As a result, we included this audit in our *Fiscal Year 2022 Audit Plan.* Our audit objective was to assess whether GSA's RPA program complies with federal and Agency information technology (IT) security policies, procedures, standards, and guidance.

What We Found

GSA should strengthen the security of its RPA program. We found that GSA's RPA program did not comply with its own IT security requirements to ensure that bots are operating securely and properly. GSA also did not consistently update system security plans to address access by bots. Instead of addressing these issues, RPA program management simply removed or modified the requirements. Lastly, GSA's RPA program did not establish an access removal process for decommissioned bots, resulting in prolonged, unnecessary access that placed GSA systems and data at risk of exposure.

[1] Office of Management and Budget Memorandum M-18-23, *Shifting from Low-Value to High-Value Work* (August 27, 2018).

[2] The Federal RPA Community of Practice consists of more than 1,400 members from over 100 federal departments and agencies.

What We Recommend

We recommend that GSA's Chief Financial Officer and Chief Information Officer:

1. Conduct a comprehensive assessment of GSA's CIO-IT Security-19-97, *IT Security Procedural Guide: Robotic Process Automation (RPA) Security*, (RPA policy) to ensure, among other things, that its monitoring controls are effectively designed and implemented.
2. Develop oversight mechanisms to enforce compliance with the RPA policy and ensure that controls are operating effectively.
3. Require system security plans to be updated as part of the RPA security approval process to address bot and non-person entity access.
4. Review all system security plans that bots currently interact with to determine if they address bot and non-person entity access. Update the system security plans, as needed.
5. Establish procedures as part of the RPA security approval process that ensure system owners consider updating the security controls identified in Appendix A of the RPA policy.
6. Review all system security plans that bots currently interact with to determine if the security controls need to be updated. Update the system security plans, as needed.
7. Develop a comprehensive process for removing bot custodian and bot developer access for decommissioned bots and GSA systems that:
    a. Aligns with GSA's CIO-IT Security-01-07, *IT Security Procedural Guide: Access Control (AC)* (access control policy);
    b. Tracks and documents that access has been removed; and
    c. Incorporates the process into the RPA policy.

In their response to our report, the Chief Financial Officer and Chief Information Officer agreed with our recommendations but did not entirely agree with our finding. The comments are included in their entirety in ***Appendix D***.

Table of Contents

Introduction

We performed an audit of GSA's robotic process automation (RPA) program because of the unique risks bots pose to GSA's systems and data.

Purpose

GSA established its RPA program to automate low-value, routine tasks, allowing its employees to spend more time on challenging work. While RPA offers the potential to save time and improve productivity, the bots' ability to perform thousands of read, write, and deletion actions at high rates of speed can make it difficult to identify logic and processing errors—and their associated consequences—before serious damage is done. As a result, we included this audit in our *Fiscal Year 2022 Audit Plan.*

Objective

The objective of our audit was to assess whether GSA's RPA program complies with federal and Agency information technology (IT) security policies, procedures, standards, and guidance.

See ***Appendix A*** – Objective, Scope, and Methodology for additional details.

Background

RPA uses bots to simulate human actions to reduce repetitive administrative tasks. These bots interact with existing systems to copy data, fill in forms, sign into applications, and send emails. In 2018, the Office of Management and Budget recommended that federal agencies use RPA as a new technological tool to shift resources from low-value to high-value work.[3] GSA began implementing RPA that same year.

GSA's RPA program is comprised of two groups:

- The Office of GSA IT's Office of Digital Infrastructure Technologies develops and deploys bots for its office.
- The Office of the Chief Financial Officer develops and deploys bots for the rest of GSA.

By December 2022, GSA had 119 active bots and 24 decommissioned bots. Decommissioned bots are those that are no longer needed or used by the RPA program.

While RPA offers significant benefits, bots pose unique risks to GSA's systems and data. Bots can perform thousands of read, write, and deletion actions at high rates of speed. This can make it difficult to identify logic and processing errors—and their associated consequences—

[3] Office of Management and Budget Memorandum M-18-23.

before serious damage is done. For example, a bot could erroneously delete or overwrite thousands of records before GSA could even identify that an issue has occurred. Because bots have access to extensive amounts of data, including sensitive data, they can pose significant security risks arising from potential data exposure. Additionally, bots interact with existing GSA systems, making it critical to establish a robust RPA security environment to protect the bots, the data they interact with, and the Agency's systems.

Prior GSA Office of Inspector General Report on GSA's Use of RPA

In November 2023, we reported that GSA lacked evidence to support its claims that its RPA program is generating savings.[4] We found that GSA was not verifying the actual work hours saved with end-users of its bots. Because of this, GSA's assertion in its Fiscal Year 2020 *Agency Financial Report* that its RPA program reclaimed more than 240,000 work hours annually was inaccurate and unreliable. We also found that GSA was not tracking the costs associated with its bots, which precludes GSA from determining whether the bots are generating cost savings and a return on investment.

Based on our finding, we recommended that GSA establish a performance evaluation process for its bots to ensure they are performing as intended and that the RPA program is achieving its goals. We also recommended that GSA track the costs to develop each bot to allow the RPA program to develop objective statistics, such as return on investment. GSA acknowledged our finding and recommendations.

[4] *GSA's Robotic Process Automation Program Lacks Evidence to Support Claimed Savings* (Report Number A210057/B/5/F24001, November 30, 2023).

Results

Finding – GSA should strengthen the security of its RPA program.

GSA should strengthen the security of its RPA program. We found that GSA's RPA program did not comply with its own IT security requirements to ensure that bots are operating securely and properly. GSA also did not consistently update system security plans to address access by bots. Instead of addressing these issues, RPA program management simply removed or modified the security requirements. Lastly, GSA's RPA program did not establish an access removal process for decommissioned bots, resulting in prolonged, unnecessary access that placed GSA systems and data at risk of exposure.

GSA's RPA Program Did Not Comply with IT Security Requirements to Ensure That Bots Operate Securely and Properly

Bots use GSA systems and data to rapidly process significant volumes of actions. Accordingly, it is critical to monitor the performance of bots to identify and correct any security or operational deficiencies in a timely manner. While GSA's RPA program had IT security requirements to ensure that its bots were operating securely and properly, it did not comply with these requirements.

The Federal RPA Community of Practice's *EXECUTIVE GUIDE Creating a Robust Controls System for RPA Programs,* recommends using a robust monitoring system to identify and resolve RPA operational errors.[5] Additionally, the Chief Information Officers Council's *Robotic Process Automation in Federal Agencies* stresses the importance of effective RPA governance, noting that bots can cause security risks and governance problems.[6] In line with these requirements, GSA's CIO-IT Security-19-97, *IT Security Procedural Guide: Robotic Process Automation (RPA) Security*, (RPA policy) required the RPA program to monitor and review the tasks performed by bots. These requirements were designed to ensure security and identify logic and processing errors.

However, the RPA program did not complete the following security monitoring requirements:

- **Baseline Monitoring –** GSA's RPA policy required management to establish and perform baseline monitoring of bots to ensure they were operating and performing as expected. Baseline monitoring was intended to provide the minimum level of monitoring required to alert RPA program management if a bot was accessing, reading, writing, or moving

[5] Federal RPA Community of Practice, *EXECUTIVE GUIDE Creating a Robust Controls System for RPA Programs,* Version 1.0 (June 25, 2020).

[6] The Chief Information Officers Council is a forum of federal chief information officers whose goal is to improve IT practices across government agencies.

more data than authorized. However, the RPA program never developed the ability to perform baseline monitoring.

- **Weekly Log Reviews –** GSA's RPA policy required bot custodians, who run and execute the bots, to perform weekly reviews of RPA activity logs. Much like baseline monitoring, these weekly reviews were intended to identify logic or processing errors in the operation of each bot. However, RPA program management told us that bot custodians were never granted access to bot logs and thus were unable to perform weekly log reviews.

- **Bot Annual Reviews –** GSA's RPA policy required the RPA program to perform a comprehensive annual review of each bot's security controls and activities. These reviews were intended to approve each bot for continued use on GSA's systems. The reviews also could have helped RPA program management identify, assess, and address any security concerns or changes to the bot. However, the RPA program did not complete bot annual reviews.

RPA program management and staff told us that many of the IT security requirements in the RPA policy were not realistic and should not have been included in the policy. Accordingly, rather than taking steps to ensure compliance with these IT security requirements, the information systems security manager for GSA's RPA systems told us that they would remove or modify them. In February 2023, GSA published the revised RPA policy, which was approved by the Chief Information Security Officer.[7] In the revised RPA policy, GSA eliminated the baseline monitoring, weekly log reviews, and bot annual reviews.

Because of the significant risks RPA poses to GSA systems and data, GSA should take a more comprehensive approach to addressing IT security for its RPA program. GSA should also conduct a complete assessment of its RPA policy to ensure, among other things, that its monitoring controls are effectively designed and implemented. GSA should then enforce compliance to ensure that the controls are operating effectively.

GSA Did Not Consistently Update System Security Plans to Address RPA Access

System security plans describe how an IT system's security controls are designed to ensure the system is protected from threats and vulnerabilities. Accordingly, these plans must identify all data flows and connections to and from the system, including those attributable to RPA. However, GSA's system security plans were not consistently updated to address how bots access the systems.

The National Institute of Standards and Technology's (NIST's) *Guide for Developing Security Plans for Federal Information Systems* states that system security plans should be maintained to

[7] The Chief Information Security Officer is responsible for GSA-wide compliance with federal security requirements.

reflect the current operating environment.[8] This ensures that associated security assessments are comprehensive and that established controls adequately protect systems. GSA Order CIO 2100.1P, *GSA Information Technology (IT) Security Policy*, requires system security plans to document all data flows to effectively manage cybersecurity risk.[9]

GSA's RPA policy required system security plans to address the system's interaction with bots. Specifically, the RPA policy required system security plans to include a listing of all bots that interact with the system and identify associated data flows. The plans must also include information about bots for specific IT controls "when Bot-specific actions, attribution, or interaction can be ascertained."[10] In accordance with GSA's CIO-IT Security-01-07, *IT Security Procedural Guide: Access Control (AC)* (access control policy), the plans must also be updated to address access by non-person entity accounts, which are non-human users that GSA uses to run bots on its systems.

We reviewed the system security plans for 16 GSA systems that are accessed by bots and found the following:[11]

- None of the 16 system security plans were updated in accordance with the RPA policy to address how bots were accessing the systems;
- 7 of the 16 system security plans did not even mention bots, thus providing no evidence that bots were even interacting with the systems; and
- 10 of the 16 system security plans failed to list and authorize non-person entities' access to the systems.

The system security plans were incomplete because they did not consistently identify bot access. This prevented GSA from ensuring that the appropriate controls were in place to protect the systems and data from the risk of exposure.

When GSA learned of the deficiencies in its system security plans during our audit, it removed the requirement to update the system security plans from its RPA policy. Instead of addressing the deficiencies, GSA revised the RPA policy by changing the requirement to update system security plans to "suggested actions." When we asked GSA management why they removed the requirement, the information systems security manager for GSA's RPA systems stated that the security controls should be updated at the discretion of system staff and only if necessary.

While system staff are ultimately responsible for updating system security plans, RPA program management are uniquely positioned to identify the relationships between bots and the

[8] NIST Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems* (February 2006).

[9] GSA Order CIO 2100.1P, *GSA Information Technology (IT) Security Policy* (January 31, 2024).

[10] See ***Appendix B*** for a listing of the IT security controls specified in GSA's RPA policy.

[11] See ***Appendix C*** for a listing of the 16 system security plans we reviewed.

systems they access. Accordingly, RPA program management should ensure that system staff are aware of and consider information about bots in their system security plans, specifically for the IT controls listed in the RPA policy.

Furthermore, although the RPA policy required RPA program management to ensure that system security plans were updated to address bot access, they failed to do so. The information systems security manager and information systems security officer for GSA's RPA systems said this was out of the scope of the RPA program management's responsibilities, resources, and authority.[12] However, both the Chief Information Security Officer and the information systems security manager for GSA's RPA systems later agreed that the RPA program should track that system security plans are updated to address bot access.

System security plans are a critical component of an effective IT security control environment; however, GSA did not ensure that these plans addressed how bots were accessing its systems. To protect its systems and data from exposure, GSA should require system security plans to address bot access and ensure that the plans are updated accordingly.

GSA's RPA Program Did Not Establish a Process to Remove Access to Decommissioned Bots

Bot custodians run and execute the bots that were designed by the bot developers. To perform these functions, the bot custodians and bot developers have access to the bots as well as to the data and systems used by the bots. Bots access a vast array of data maintained in GSA systems. This data includes sensitive information, such as controlled unclassified information and personally identifiable information (PII). Accordingly, it is critical that effective processes are in place to protect this data from unauthorized access. However, we found that the RPA program did not establish processes to:

- Remove bot custodians' and bot developers' access to bots and their associated GSA systems when bots were decommissioned; and
- Clearly document access removal to bots and their associated GSA systems.

Taken together, these deficiencies resulted in prolonged, unnecessary access to bots and their associated GSA systems, placing the systems and data at risk of exposure.

GSA did not establish a process to ensure that bot custodians' and bot developers' access was removed for decommissioned bots and their associated GSA systems. Bot custodians run and execute the bots that were designed by the bot developers. When a bot is decommissioned, bot custodians and bot developers no longer need access to the bots and their associated GSA systems and data. Accordingly, their accounts should be disabled or removed. However, the

[12] The information systems security manager is responsible for all IT system security and privacy matters for the system under their purview. Information systems security officers report to the information systems security manager and are responsible for ensuring implementation of adequate system security.

RPA program did not establish a process to ensure bot custodians and bot developers had their access removed for decommissioned bots, resulting in unnecessary and prolonged access.

Sound IT security management provides that accounts should be disabled or removed in a timely manner when the account holder no longer has a business need to access the system. GSA's access control policy requires notifying account managers within 14 days when accounts are no longer required. The access control policy also states that GSA should limit "user access only to needed information required to perform specific responsibilities…."

As described below, we found that GSA did not remove bot custodians' and bot developers' access for decommissioned bots in a timely manner or did not do so at all.

Bot custodians. GSA did not remove access for almost all bot custodians in a timely manner after the bots were decommissioned. GSA assigned 56 bot custodians to its 24 decommissioned bots. However, we found that GSA did not remove access for 55 out of these 56 bot custodians within the 14-day period prescribed by GSA's access control policy. For example, GSA did not remove access for two bot custodians assigned to a bot that handled PII, including social security numbers, for over 4 months after the bot was decommissioned. In another example, GSA did not remove access for seven bot custodians assigned to a bot that handled similar PII for almost 10 months after the bot was decommissioned.

Of the 55 bot custodians whose access was not removed in a timely manner, 8 still had access to a decommissioned bot at the time of our audit. When we informed RPA program management of this deficiency, they promptly removed access for the eight bot custodians.

Bot developers. GSA used 13 bot developers for its 24 decommissioned bots. However, according to the RPA Program Director, GSA did not remove bot developers' access to any decommissioned bots and their associated GSA systems and data. These bots accessed GSA systems that contain a variety of sensitive data, including controlled unclassified information, PII, financial information, and procurement-sensitive information.

The RPA Program Director said they did not establish an access removal process because they did not consider how to decommission bots when establishing the RPA program. As a result of our audit, RPA program management developed an access removal process for bot custodians in June 2023. The process establishes a 30-day time frame to remove bot custodian access after GSA determines a bot is no longer needed.

However, the time frame does not align with GSA's access control policy, is not documented in the RPA policy, and only applies to bot custodians—it does not apply to bot developers. Accordingly, GSA should develop a comprehensive process that aligns with GSA's access control policy for the timely removal of access for decommissioned bots and incorporate it into its RPA policy.

GSA did not establish a process to document access removal to bots and their associated systems. NIST's *Security and Privacy Controls for Federal Information Systems and Organizations* requires GSA to log events, including account management and access removal, that are significant and relevant to system security.[13] Effective event logging is an important part of an organization's monitoring and auditing capability and can be used to help identify the root cause of problems. However, the RPA program did not establish a process to clearly document the removal of access to bots and their associated GSA systems, which prevented the program from confirming that access was removed in a timely manner. As a result, the RPA program had incomplete and conflicting access removal documentation.

For example, we found that the RPA program could not provide documentation confirming access to decommissioned bots was removed for three bot custodians. RPA program management also provided conflicting documentation, which affected not only the reliability of the program's records, but also RPA program management's ability to confirm when and if access had been removed. Some access removal documents listed the bot custodians, while others failed to do so. This made it difficult to determine who had access to GSA's bots.

RPA program management said they requested access removal through informal and undocumented communication channels; however, they acknowledged the need to formally document these requests and maintain accurate access removal records. GSA should establish procedures to document and track that access has been removed.

[13] NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations* (September 2020).

Conclusion

GSA should strengthen the security of its RPA program. We found that GSA’s RPA program did not comply with its own IT security requirements to ensure that bots are operating securely and properly. GSA also did not consistently update system security plans to address access by bots. Instead of addressing these issues, RPA program management simply removed or modified the requirements. Lastly, GSA’s RPA program did not establish an access removal process for decommissioned bots, resulting in prolonged, unnecessary access that placed GSA systems and data at risk of exposure.

Throughout our audit, GSA’s RPA program management made changes to IT security controls and told us that they did so in response to our audit inquiries. In some cases, RPA program management chose to weaken controls rather than ensure that existing controls were followed. Furthermore, these changes were only made in reaction to our audit and not based on a comprehensive assessment to ensure that the changes most appropriately met the needs of the RPA program and protected GSA systems and data. Accordingly, in addition to addressing the specific finding of our report, we recommend that GSA conduct a thorough assessment of its RPA security controls to ensure they are designed and operating effectively.

Recommendations

We recommend that GSA’s Chief Financial Officer and Chief Information Officer (CIO):

1. Conduct a comprehensive assessment of GSA’s CIO-IT Security-19-97, *IT Security Procedural Guide: Robotic Process Automation (RPA) Security,* (RPA policy) to ensure, among other things, that its monitoring controls are effectively designed and implemented.
2. Develop oversight mechanisms to enforce compliance with the RPA policy and ensure that controls are operating effectively.
3. Require system security plans to be updated as part of the RPA security approval process to address bot and non-person entity access.
4. Review all system security plans that bots currently interact with to determine if they address bot and non-person entity access. Update the system security plans, as needed.
5. Establish procedures as part of the RPA security approval process that ensure system owners consider updating the security controls identified in Appendix A of the RPA policy.
6. Review all system security plans that bots currently interact with to determine if the security controls need to be updated. Update the system security plans, as needed.

7. Develop a comprehensive process for removing bot custodian and bot developer access for decommissioned bots and GSA systems that:
    a. Aligns with GSA's CIO-IT Security-01-07, *IT Security Procedural Guide: Access Control (AC)* (access control policy);
    b. Tracks and documents that access has been removed; and
    c. Incorporates the process into the RPA policy.

GSA Comments

The GSA Chief Financial Officer and CIO agreed with our recommendations but did not entirely agree with our finding. GSA also provided technical comments to our report. The comments are included in their entirety in ***Appendix D***. We summarize and respond to GSA's technical comments below. For the reasons described in our responses, we reaffirm our finding and conclusions.

1. GSA offered a "Factual Clarification" to our description of the unique risks that bots pose to GSA's systems and data in the *Background* section of the report. Specifically, we noted that the bots' ability to perform thousands of read, write, and deletion actions at high rates of speed can make it difficult to identify logic and processing errors—and their associated consequences—before serious damage is done. GSA responded that it "has controls in place that would make it technically impossible for a bot to erroneously delete thousands of records before GSA has identified that an issue has occurred." GSA also provided a brief description of its controls.

   OIG Response: Our description of the unique risks associated with bots was based on risks described in the *EXECUTIVE GUIDE Creating a Robust Controls System for RPA Programs* (Executive Guide), which was issued in June 2020 by the GSA-established Federal RPA Community of Practice. The Executive Guide identifies general risks facing RPA programs. For example, the guide states the following:

   > Individual RPA automations can potentially process batches of tens of thousands of transactions. The impact of flawed logic and processing errors will have significant impact. The time and energy required to investigate, evaluate and re-work processing errors can create significant workloads for RPA program and business staff.

   We summarized this and other provisions of the Executive Guide in our report as background information to provide context on the need for effective controls to protect against these risks. It is not an audit finding. Nonetheless, while GSA asserts that its "security controls ensure that the RPA environment is protected and do not allow an RPA managed bot to delete or overwrite data unless specifically programmed to do so," our audit finding shows that opportunities exist to strengthen the security of GSA's RPA program.

2. GSA offered “additional context” to our finding that the Agency removed or modified IT security requirements in the RPA policy rather than taking steps to enforce the requirements. GSA acknowledged that updates were made and wrote that “the updates ensured bots operate securely initially and on an ongoing basis.”

   OIG Response: In our report, we note that because of the significant risks RPA poses to GSA systems and data, GSA should take a more comprehensive approach to addressing IT security for its RPA program. However, during our audit, we found that rather than taking a comprehensive approach to IT security, GSA eliminated IT security requirements as we brought instances of noncompliance to management’s attention.

3. GSA provided context for its decision to remove the requirement to update system security plans to address the system’s interaction with bots. However, GSA added that based on our finding that the system security plans were not consistently updated, it will revise its policy to again require that system security plans address the system’s interaction with bots.

   OIG Response: As provided in our report, system security plans describe how an IT system’s security controls are designed to ensure the system is protected from threats and vulnerabilities. These plans must identify all data flows and connections to and from the system, including those attributable to RPA.

4. Responding to our finding that GSA’s RPA program did not establish a process to remove access to decommissioned bots, GSA wrote that its access control policy only requires notification to account managers within 14 days when bot custodians’ and bot developers’ accounts are no longer required. GSA added that it “disables bots in a timely manner when bots are no longer required (following notifications from process owners) which mitigates the risk of accessing decommissioned bots.” Nonetheless, GSA wrote that it “acknowledges that its access removal practices should be improved….”

   OIG Response: As provided in our report, it is critical that effective processes are in place to protect GSA data from unauthorized access, including access to decommissioned bots. However, we found that a significant number of bot custodians and developers maintained access to decommissioned bots and their associated systems and data.

Audit Team

This audit was managed out of the Information Technology Audit Office and conducted by the individuals listed below:

Sonya Panzo	Associate Deputy Assistant Inspector General for Auditing
Kyle Plum	Audit Manager
James Dean	Auditor-In-Charge

Appendix A – Objective, Scope, and Methodology

Objective

We performed an audit of GSA's RPA program because of the unique risks bots pose to GSA's systems and data. The objective of our audit was to assess whether GSA's RPA program complies with federal and Agency IT security policies, procedures, standards, and guidance.

Scope and Methodology

We assessed the RPA program's compliance with federal and Agency IT security policies, procedures, standards, and guidance.

To accomplish our objective, we:

- Reviewed federal and GSA policies and guidance for RPA programs and IT security, including:
  - Office of Management and Budget Memorandum M-18-23, *Shifting from Low-Value to High-Value Work* (August 27, 2018);
  - NIST Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems* (February 2006);
  - NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations* (September 2020);
  - GSA Order CIO 2100.1P, *GSA Information Technology (IT) Security Policy* (January 31, 2024);
  - CIO-IT Security-01-07, Revision 5, *IT Security Procedural Guide: Access Control (AC)* (August 18, 2022);
  - CIO-IT Security-19-97, Revision 2, *IT Security Procedural Guide: Robotic Process Automation (RPA) Security* (March 31, 2020);
  - CIO-IT Security-19-97, Revision 3, *IT Security Procedural Guide: Robotic Process Automation (RPA) Security* (February 14, 2023);
  - Chief Information Officers Council, *Robotic Process Automation in Federal Agencies* (undated); and
  - The Federal RPA Community of Practice, *EXECUTIVE GUIDE Creating a Robust Controls System for RPA Programs,* Version 1.0 (June 25, 2020);
- Assessed the RPA program's procedures to determine compliance or identify deficiencies with CIO-IT Security-19-97, Revision 2;
- Obtained and reviewed GSA's system security plans for systems that bots interact with. See ***Appendix C*** for a list of system security plans we reviewed;
- Obtained and analyzed the RPA program's access removal data for the entire population of 24 decommissioned bots, including their associated non-person entity accounts and bot custodians; and

- Interviewed the Chief Information Security Officer, RPA program officials, and RPA program staff.

Data Reliability

We assessed the reliability of access removal data for decommissioned bots provided by the RPA program. This data included names of bot custodians and bot developers, their access to specific bots, and the date their access was removed. We interviewed RPA program management and observed system demonstrations to better understand the data. We determined that the data was sufficiently reliable for the purposes of this audit.

Sampling

We selected a judgmental sample of 20 out of the 119 active bots GSA had in December 2022 and compiled a listing of GSA's Federal Information Security Modernization Act of 2014 (FISMA) systems that these bots interacted with. We determined that our judgmental sample of bots interacted with a total of 16 systems. We reviewed the system security plans for these 16 systems (see ***Appendix C***) to determine if they addressed bot access.

Our judgmental sample of 16 GSA systems does not allow for projection to the entire population of GSA's 21 FISMA systems that interact with bots. However, our sample did allow us to adequately address our audit objective and make recommendations.

Internal Controls

We assessed internal controls significant within the context of our audit objective against GAO-14-704G, *Standards for Internal Control in the Federal Government*. The methodology above describes the scope of our assessment, and the report finding includes any internal control deficiencies we identified. Our assessment is not intended to provide assurance on GSA's internal control structure as a whole. GSA management is responsible for establishing and maintaining internal controls.

Compliance Statement

We conducted the audit between October 2022 and March 2024 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our finding and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our finding and conclusions based on our audit objective.

Appendix B – GSA's Instructions for Updating Security Controls in the Agency's System Security Plans[14]

The following table is a re-creation of *Table A-1: Instructions on NIST Control Implementation Regarding BOTs* from GSA's RPA policy.

NIST Control	FIPS Levels[15]	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.
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.[16]

[14] CIO-IT Security-19-97, *IT Security Procedural Guide: Robotic Process Automation (RPA) Security,* Revision 2 (March 31, 2020).

[15] NIST's Federal Information Processing Standards (FIPS) Publication 199 establishes three security categorizations that are based on the potential impact (i.e., L=Low, M=Moderate, or H=High impact) on an organization should events occur that jeopardize the information system.

[16] MFA refers to multi-factor authentication.

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.

Appendix C – Population of Reviewed FISMA System Security Plans

Below is a list of system descriptions for the 16 system security plans we reviewed.[17] This list contains the information system name and abbreviation as documented in the system security plan.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[17] Redactions represent sensitive IT security information.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

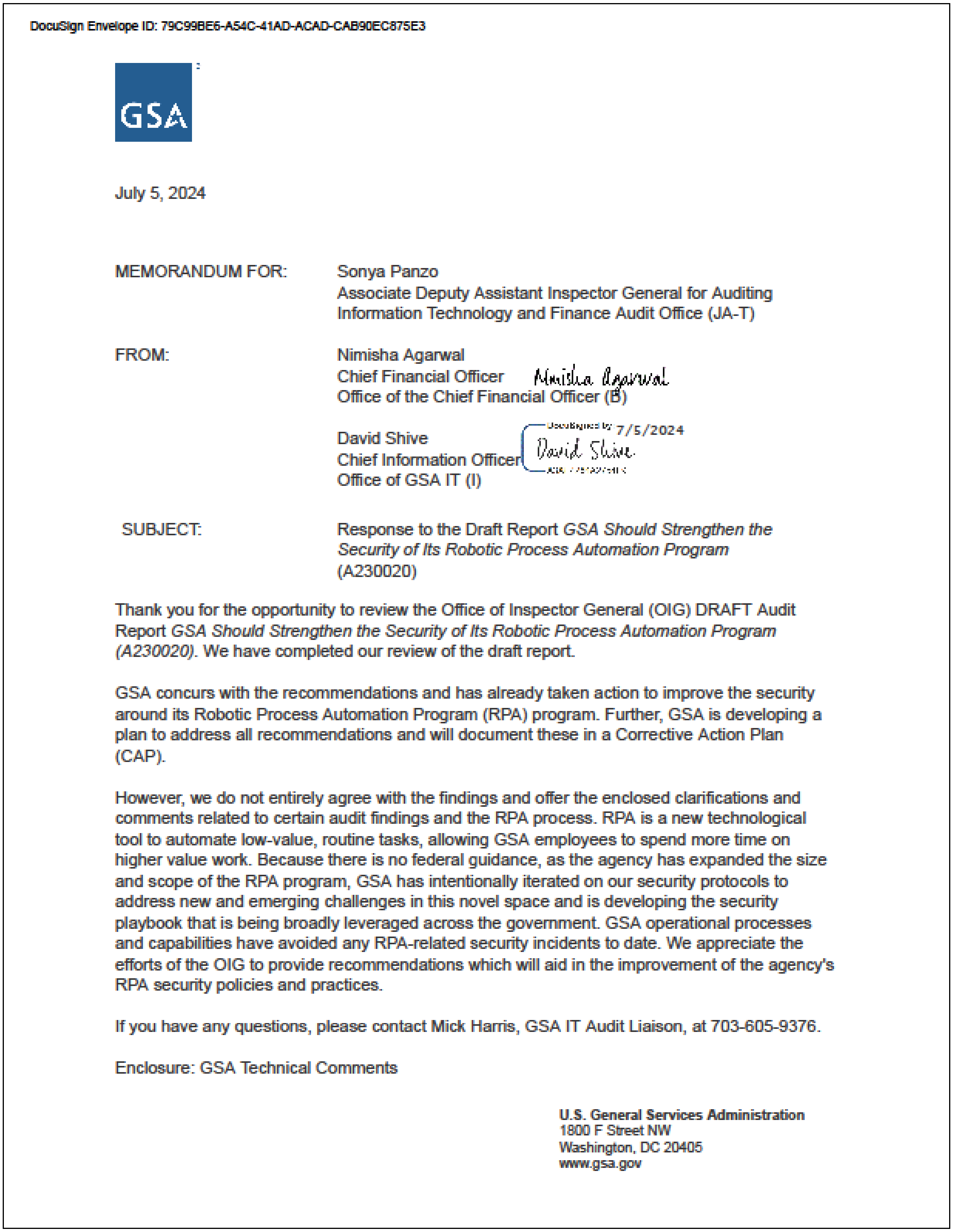
[redacted]

[redacted]

[redacted]

[redacted]

Appendix D – GSA Comments



DocuSign Envelope ID: 79C99BE6-A54C-41AD-ACAD-CAB90EC875E3

GSA

July 5, 2024

MEMORANDUM FOR: Sonya Panzo
Associate Deputy Assistant Inspector General for Auditing
Information Technology and Finance Audit Office (JA-T)

FROM: Nimisha Agarwal
Chief Financial Officer
Office of the Chief Financial Officer (B)

Nimisha Agarwal

David Shive
Chief Information Officer
Office of GSA IT (I)

DocuSigned by: 7/5/2024
David Shive
[illegible]

SUBJECT: Response to the Draft Report *GSA Should Strengthen the Security of Its Robotic Process Automation Program* (A230020)

Thank you for the opportunity to review the Office of Inspector General (OIG) DRAFT Audit Report *GSA Should Strengthen the Security of Its Robotic Process Automation Program (A230020)*. We have completed our review of the draft report.

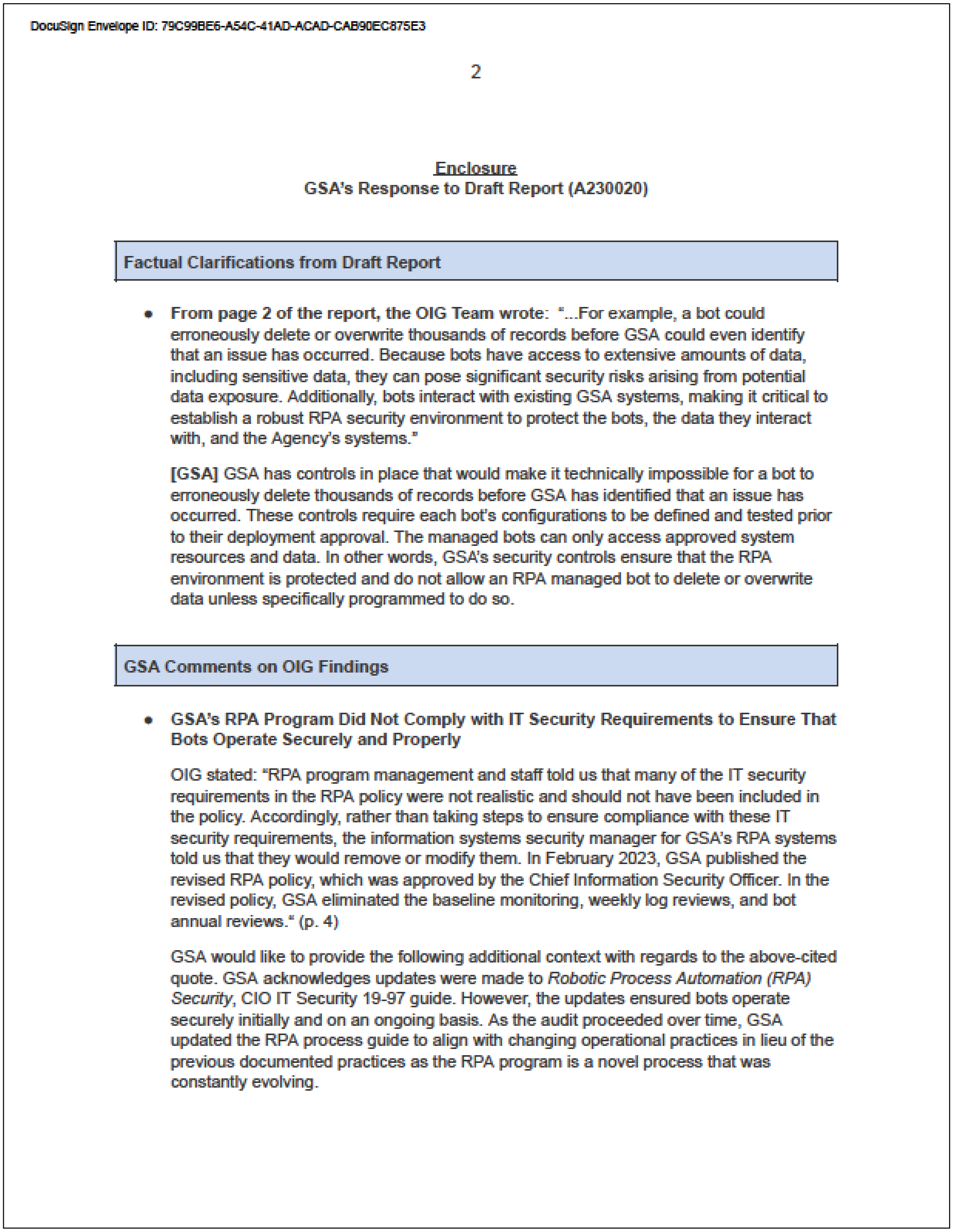
GSA concurs with the recommendations and has already taken action to improve the security around its Robotic Process Automation Program (RPA) program. Further, GSA is developing a plan to address all recommendations and will document these in a Corrective Action Plan (CAP).

However, we do not entirely agree with the findings and offer the enclosed clarifications and comments related to certain audit findings and the RPA process. RPA is a new technological tool to automate low-value, routine tasks, allowing GSA employees to spend more time on higher value work. Because there is no federal guidance, as the agency has expanded the size and scope of the RPA program, GSA has intentionally iterated on our security protocols to address new and emerging challenges in this novel space and is developing the security playbook that is being broadly leveraged across the government. GSA operational processes and capabilities have avoided any RPA-related security incidents to date. We appreciate the efforts of the OIG to provide recommendations which will aid in the improvement of the agency's RPA security policies and practices.

If you have any questions, please contact Mick Harris, GSA IT Audit Liaison, at 703-605-9376.

Enclosure: GSA Technical Comments

U.S. General Services Administration
1800 F Street NW
Washington, DC 20405
www.gsa.gov



Enclosure
GSA's Response to Draft Report (A230020)

Factual Clarifications from Draft Report

- **From page 2 of the report, the OIG Team wrote:** "...For example, a bot could erroneously delete or overwrite thousands of records before GSA could even identify that an issue has occurred. Because bots have access to extensive amounts of data, including sensitive data, they can pose significant security risks arising from potential data exposure. Additionally, bots interact with existing GSA systems, making it critical to establish a robust RPA security environment to protect the bots, the data they interact with, and the Agency's systems."

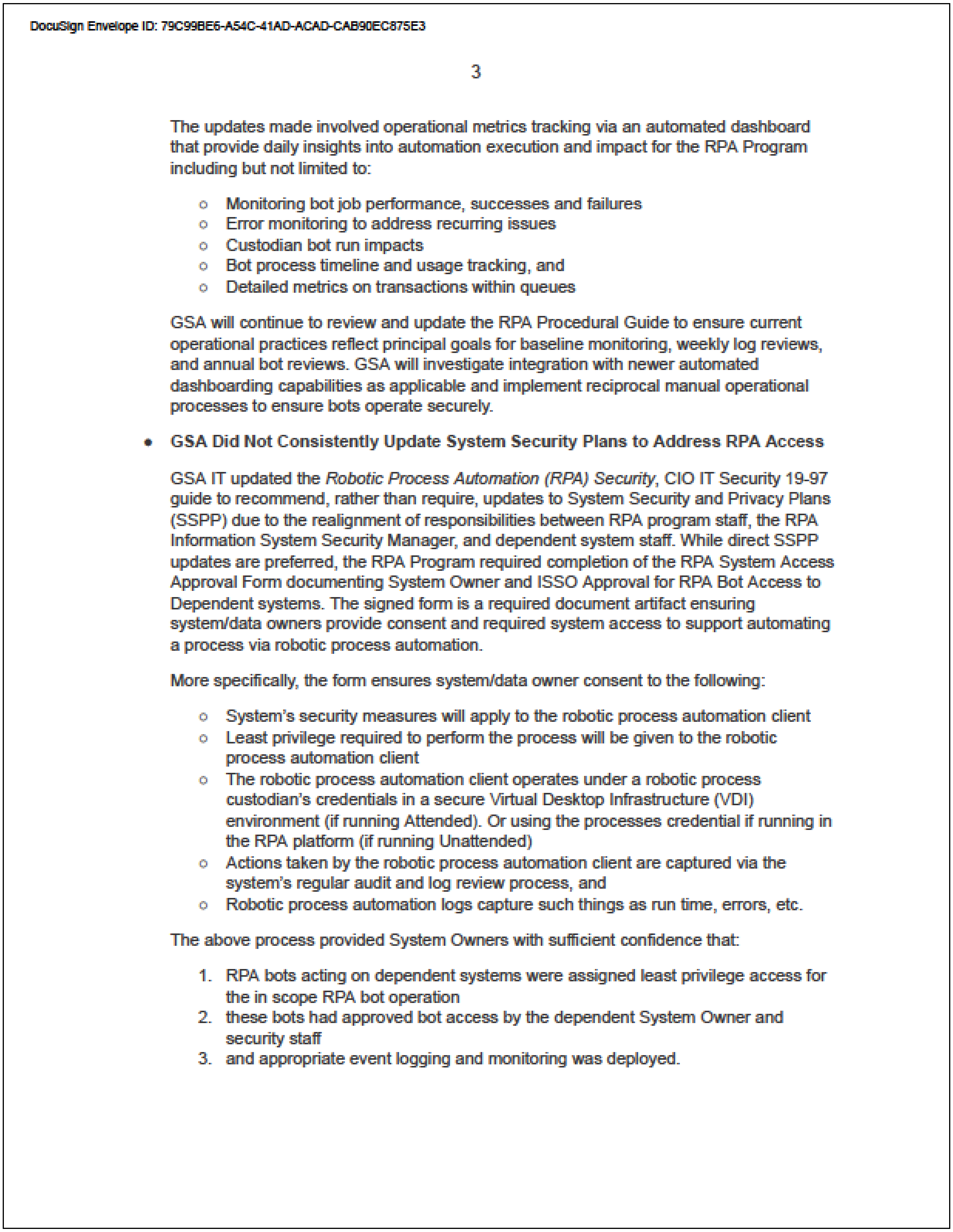
  [GSA] GSA has controls in place that would make it technically impossible for a bot to erroneously delete thousands of records before GSA has identified that an issue has occurred. These controls require each bot's configurations to be defined and tested prior to their deployment approval. The managed bots can only access approved system resources and data. In other words, GSA's security controls ensure that the RPA environment is protected and do not allow an RPA managed bot to delete or overwrite data unless specifically programmed to do so.

GSA Comments on OIG Findings

- **GSA's RPA Program Did Not Comply with IT Security Requirements to Ensure That Bots Operate Securely and Properly**

  OIG stated: "RPA program management and staff told us that many of the IT security requirements in the RPA policy were not realistic and should not have been included in the policy. Accordingly, rather than taking steps to ensure compliance with these IT security requirements, the information systems security manager for GSA's RPA systems told us that they would remove or modify them. In February 2023, GSA published the revised RPA policy, which was approved by the Chief Information Security Officer. In the revised policy, GSA eliminated the baseline monitoring, weekly log reviews, and bot annual reviews." (p. 4)

  GSA would like to provide the following additional context with regards to the above-cited quote. GSA acknowledges updates were made to *Robotic Process Automation (RPA) Security*, CIO IT Security 19-97 guide. However, the updates ensured bots operate securely initially and on an ongoing basis. As the audit proceeded over time, GSA updated the RPA process guide to align with changing operational practices in lieu of the previous documented practices as the RPA program is a novel process that was constantly evolving.



The updates made involved operational metrics tracking via an automated dashboard that provide daily insights into automation execution and impact for the RPA Program including but not limited to:

- Monitoring bot job performance, successes and failures
- Error monitoring to address recurring issues
- Custodian bot run impacts
- Bot process timeline and usage tracking, and
- Detailed metrics on transactions within queues

GSA will continue to review and update the RPA Procedural Guide to ensure current operational practices reflect principal goals for baseline monitoring, weekly log reviews, and annual bot reviews. GSA will investigate integration with newer automated dashboarding capabilities as applicable and implement reciprocal manual operational processes to ensure bots operate securely.

- **GSA Did Not Consistently Update System Security Plans to Address RPA Access**

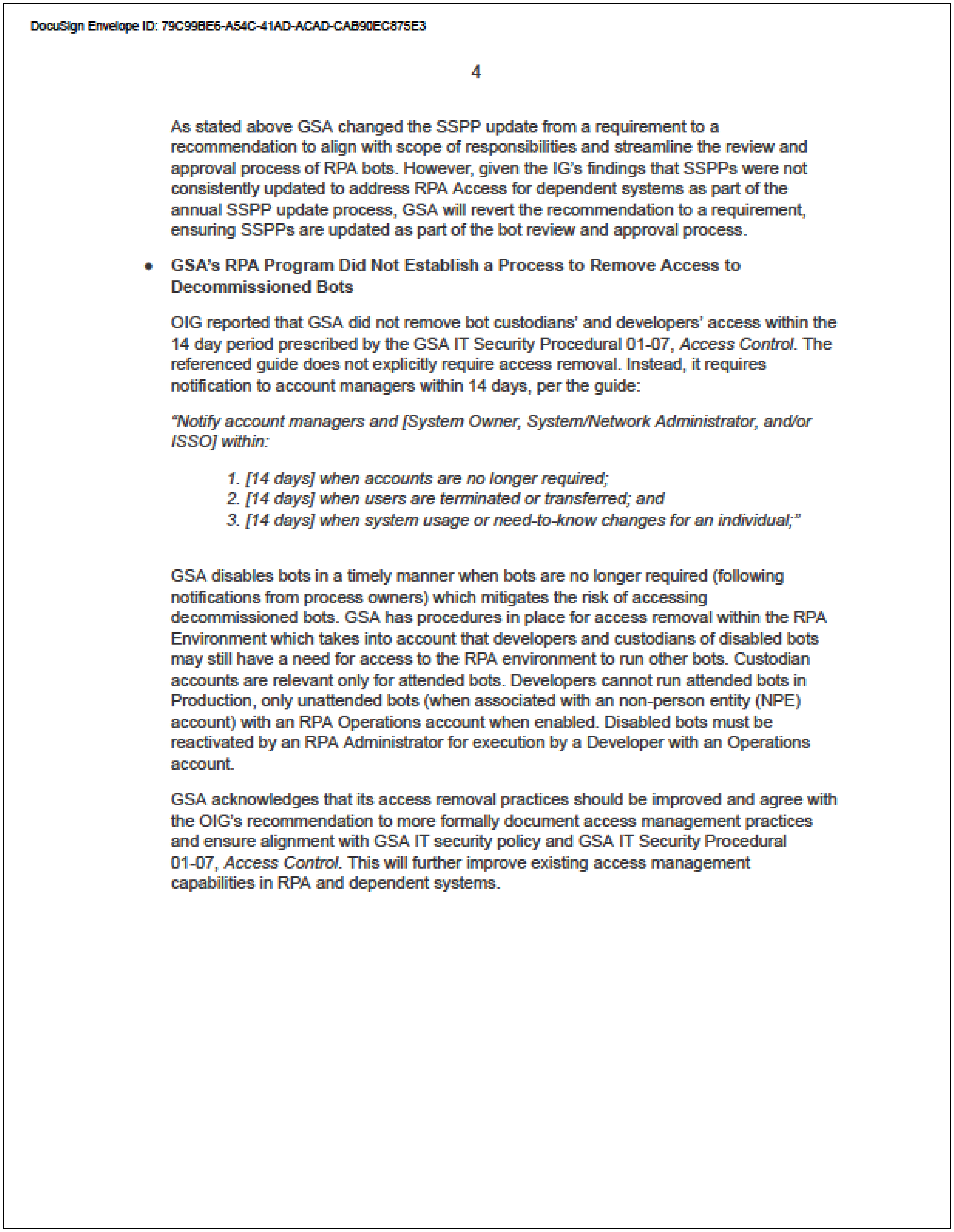
GSA IT updated the *Robotic Process Automation (RPA) Security*, CIO IT Security 19-97 guide to recommend, rather than require, updates to System Security and Privacy Plans (SSPP) due to the realignment of responsibilities between RPA program staff, the RPA Information System Security Manager, and dependent system staff. While direct SSPP updates are preferred, the RPA Program required completion of the RPA System Access Approval Form documenting System Owner and ISSO Approval for RPA Bot Access to Dependent systems. The signed form is a required document artifact ensuring system/data owners provide consent and required system access to support automating a process via robotic process automation.

More specifically, the form ensures system/data owner consent to the following:

- System's security measures will apply to the robotic process automation client
- Least privilege required to perform the process will be given to the robotic process automation client
- The robotic process automation client operates under a robotic process custodian's credentials in a secure Virtual Desktop Infrastructure (VDI) environment (if running Attended). Or using the processes credential if running in the RPA platform (if running Unattended)
- Actions taken by the robotic process automation client are captured via the system's regular audit and log review process, and
- Robotic process automation logs capture such things as run time, errors, etc.

The above process provided System Owners with sufficient confidence that:

1. RPA bots acting on dependent systems were assigned least privilege access for the in scope RPA bot operation
2. these bots had approved bot access by the dependent System Owner and security staff
3. and appropriate event logging and monitoring was deployed.



As stated above GSA changed the SSPP update from a requirement to a recommendation to align with scope of responsibilities and streamline the review and approval process of RPA bots. However, given the IG's findings that SSPPs were not consistently updated to address RPA Access for dependent systems as part of the annual SSPP update process, GSA will revert the recommendation to a requirement, ensuring SSPPs are updated as part of the bot review and approval process.

- **GSA's RPA Program Did Not Establish a Process to Remove Access to Decommissioned Bots**

OIG reported that GSA did not remove bot custodians' and developers' access within the 14 day period prescribed by the GSA IT Security Procedural 01-07, *Access Control*. The referenced guide does not explicitly require access removal. Instead, it requires notification to account managers within 14 days, per the guide:

"Notify account managers and [System Owner, System/Network Administrator, and/or ISSO] within:

1. *[14 days] when accounts are no longer required;*
2. *[14 days] when users are terminated or transferred; and*
3. *[14 days] when system usage or need-to-know changes for an individual;"*

GSA disables bots in a timely manner when bots are no longer required (following notifications from process owners) which mitigates the risk of accessing decommissioned bots. GSA has procedures in place for access removal within the RPA Environment which takes into account that developers and custodians of disabled bots may still have a need for access to the RPA environment to run other bots. Custodian accounts are relevant only for attended bots. Developers cannot run attended bots in Production, only unattended bots (when associated with an non-person entity (NPE) account) with an RPA Operations account when enabled. Disabled bots must be reactivated by an RPA Administrator for execution by a Developer with an Operations account.

GSA acknowledges that its access removal practices should be improved and agree with the OIG's recommendation to more formally document access management practices and ensure alignment with GSA IT security policy and GSA IT Security Procedural 01-07, *Access Control*. This will further improve existing access management capabilities in RPA and dependent systems.

Appendix E – Report Distribution

GSA Administrator (A)

GSA Deputy Administrator (AD)

Chief Financial Officer (B)

Acting Chief of Staff (B)

Chief Information Officer (I)

Acting Deputy Chief Information Officer (ID)

Chief of Staff (I)

Chief Information Security Officer (IS)

Robotic Process Automation Program Director (BGR)

Enterprise & Infrastructure Support Branch Chief (ISTE)

Office of Audit Management and Accountability (BA)

Assistant Inspector General for Auditing (JA)

Deputy Assistant Inspector General for Acquisition Audits (JA)

Deputy Assistant Inspector General for Real Property Audits (JA)

Director, Audit Planning, Policy, and Operations Staff (JAO)