THALES

Robotic Process Automation

Industry Insights

Robotic Process Automation (RPA) is one of many automation technologies that apply elements of Artificial Intelligence (AI) to make workflows more efficient, and shift employees away from routine tasks to higher-value forms of work. This is a rapidly-evolving space —the growing adoption of RPA in private sector enterprises is now carrying over into the public sector.

In fact, the opportunities for improving efficiencies in the public sector are so great that the adoption of technologies like RPA is being mandated. Not only do IT decision-makers for U.S. Federal agencies need to get up to speed on RPA, but they must also ensure that current levels of data security applied to humans extends to robots as well.

Key Drivers

At a high level, the rationale for RPA is clear – all businesses view automation as a way to reduce costs and make the workplace more efficient. When "intelligence" is added to automation applications – such as with RPA – the value can be even greater. Robots can perform 24/7, they don't incur additional costs, they can reduce human error, and can process information far faster than humans.

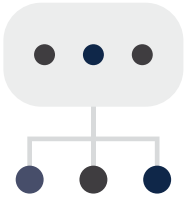
These alone would be adoption drivers for RPA, but the federal government has recently identified RPA as part of a broader initiative, the President's Management Agenda. As per Memo M-18-23 from the Office of Management and Budget, the 24 CFO Act agencies are required to follow a set of guidelines, including "developing and implementing strategies for shifting resources to high-value activities". A key element of this new strategy is to "introduce new technologies, such as RPA, to reduce repetitive administrative tasks, and other process-reform initiatives".

Aside from these workflow efficiencies, there's a related driver in terms of the federal government's labor pool. Baby Boomers represent the largest demographic in the public sector, and their ranks are diminishing as they reach retirement. To help keep the cost of government in check, these workers are not being fully replaced, which makes for a smaller labor pool overall. As workloads grow with ever-increasing volumes of data to manage, supporting today's workers is another key driver for RPA.

These all may be valid drivers for RPA, but efficiency is not the only concern of the federal government. There is a broad recognition of the need to modernize IT infrastructure, not just to manage growing volumes of data, but also to keep data secure across both premises-based and cloud-based environments.

As noted in Memo M-19-17, there is an "intensified focus on risk management...and solutions that enhance privacy and security". To address this, federal government agencies "must be able to identify, credential, monitor, and manage subjects that access Federal resources". This extends to how agencies "conduct identity proofing, establish enterprise digital identities, and adopt sound processes for authentication and access control".

Clearly, there is more to RPA than automating routine tasks. RPA is still new, and aside from being complex technology, the terminology is not yet standardized. The next section will help IT decision-makers in terms of navigating the basics, along with what's needed for robots to take on human tasks in a secure manner.



RPA Basics

As the name suggests, RPA is designed to emulate some forms of work done by humans, usually routine tasks and processes. The higher the volume, and/or the simpler the task, the greater the value of RPA. Another way that RPA brings value is the ability to perform in both digital environments (cloud-based) and legacy environments. This provides an important bridge to the future, since RPA will support today's technology upgrades, along with the extensive premises-based applications that remain in use across the public sector.

Regardless of the environment, there are two operating modes for RPA – unattended and attended. The latter applies to cases where a task or process cannot be fully automated, so the robot works in tandem with humans. Since humans can intervene at any time, these applications pose fewer security concerns. Conversely, the business value is reduced since human labor is always involved.

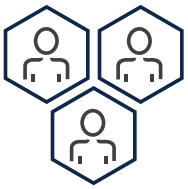
There's a larger potential payoff with unattended RPA, since there's end-to-end automation. Not only does this free-up workers for high-value tasks, but these applications can be scheduled to run at any time, or even at all times. These efficiencies are very-much aligned with the OMB mandate mentioned earlier, so it's understandable why there's so much interest in unattended RPA. In this context, RPA is poised to become a key enabler of tomorrow's digital workforce, especially for unattended applications. Keeping data secure is of the utmost importance for IT, and unattended RPA presents a distinct challenge. To date, identity management has only been for humans, so the need to support robots and other Non-Person Entities (NPEs) is quite new.

Existing forms of credentialing are PKI-based – such as smart cards – and can be extended to robots in the form of software certificates that comply with federal government requirements. These digital identity certificates can be stored onsite where the robots are hosted, or in a remote Hardware Security Module (HSM).

While all of these elements exist today, having fully secure unattended RPA – at scale – sets a high threshold for meaningful adoption to occur. Exhibiting a proof of concept is the litmus test the federal government has been waiting for, and that was demonstrated on May 6, 2019 by the Defense Logistics Agency (DLA)[1].

In DLA's use case, a robot could obtain PKI-based credentialing to gain access to DLA sites and operate around the clock. This was a first for any government agency, making both forms of RPA truly viable options for automating workflows.

Before continuing, as IT decision-makers go further down this path, many other terms will come up that are analogous to RPA. This may be confusing, as vendors tend to use their own terminology, so care should be taken with vendors for clarity. Common examples include digital workers, Intelligent Process Automation, Intelligent Business Automation, and Desktop Automation.



Key Benefits

To this point, the key benefits of RPA should be clear. Ultimately, automation is the goal, not just to improve efficiency, but also to let workers do more of what humans do best – apply critical thinking, using judgment, etc. These benefits line up nicely with the OMB's mandate, but the finer points of automation are worth noting as well, namely:

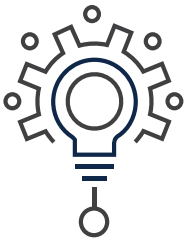
- Faster workflows – efficiency isn't just about getting more done, but also in less time
- Improved accuracy – less human error from manually copying or transcribing information
- Less duplication of work – instead of manually copying information from one source to another each time, RPA only needs to do it once
- Reduced costs – need fewer workers, less need for overtime, reduced expenses to support manual workflows
- Easier access to information – once credentialed, robots can access data faster and easier than humans
- Intuitive for digital natives – RPA will be accepted by younger workers who trust and embrace technology

Another way to assess the benefits of RPA is to consider the use cases, of which there are many. Here are some common examples that will resonate with federal government agencies:

- Automating the transfer of funds between agencies
- Standardizing employee names across various databases so it's easier to grant them access regardless of where requesting permission from
- Tracking date and time for all steps throughout a process – helps support audit requests
- Monitoring compliance when working with contractors
- Managing payment procurement across the agency supply chain
- Onboarding new employees and suppliers
- Managing and extracting data across multiple document sources and formats

https://www.fedscoop.com/defense-logistics-agency-security-rpa/

- Importing, exporting and reformatting data across multiple platforms or applications
- Automating payroll
- Report generation
- Reminders and alerts
- Issuing invoices



Implications for IT

Having demonstrated proof of concept, both modes of RPA – attended and unattended – should now be considered for use in federal agencies. There are many reasons why IT would have been reluctant to deploy robots to drive automation initiatives, but that thinking needs to change. First off, RPA isn't a strategy to displace workers and reduce staff levels. If anything, RPA will enhance employee performance, and potentially improve their level of engagement both with coworkers and the public.

Secondly, knowing that the technology is market-ready and proven now for public sector use cases, IT can focus on the biggest challenge remaining. For robots to effectively emulate humans in the workplace, they must be able to access data and applications across the organization. Furthermore, IT needs to ensure that these robots and bot applications are keeping data just as secure as with human workers.

Automation introduces new forms of risk, especially when accessing data that's based in the cloud. IT needs to be aware of the distinct cyber risks that come with RPA, along with the approaches required to ensure that bots are "who they say they are". After all, the risks can be even greater than when granting access to humans, since they generally only work no longer than eight hours at a time. When access is granted to an unattended bot, the window for security risk is larger since they can run 24/7. The following are some prime examples to consider:

- External threats where a bad actor compromises a bot to gain access to sensitive data
- Internal threats where an employee or contractor manipulates or trains a bot for malicious purposes
- Poor design where the bot inadvertently exposes sensitive data – personal information, voter registrations, financial details, etc. – to unsecure sources such as the Internet or public WiFi
- Unsecure data management, where the bot accesses sensitive data, but does not encrypt it before sending to or from the cloud
- Network vulnerability, where a poorly-designed robot enables hackers to remotely attack the network
- Denial of service interruption – this could arise if scheduled robot activities occur in such rapid succession that the network is overwhelmed, causing a ripple effect of service disruptions and possible security breaches across the organization

When developing a data security strategy for RPA, cyber risks like these – and others – need to be taken into account. This Insight Brief provides a starting point for that strategy, and once in place, IT will be much better positioned to evaluate technology partners for RPA.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled.

Contact Us: For more information, visit www.thalestct.com

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com