Securing, automating and mobilizing government workflows.

NUANCE

Executive summary

National, regional and local government agencies worldwide are not adequately dealing with the pervasive and expensive problems of security, control and access in their document—and information-related workflows.

While rightfully concerned that their private and personal information be protected as required by law or regulation, citizens everywhere want to engage with their governments in more modern, technology-based ways. At the same time, younger, more digitally literate, government employees are coming on board, anxious for new ways to create, share and apply information. Yet so much of government decision-making and service delivery still remains mired in inefficient, unsecure and wasteful paper-based processes.

Tight budgets and conflicting priorities are part of the problem. Even when governments know that their document processes are out-of-date, they are less likely than the commercial sector to allocate budgets toward fixing them. Where modernization projects do exist, according to IDC, they are budgeted at low levels.

So documents remain a leading source of expense, inefficiency and risk, even where governments have started to deploy the smart information technologies—such as multi-function devices (MFDs), mobile phones and tablet—through which they hope to realize process improvements. Unfortunately, these touch points in the modern collaborative process for document creation, access and sharing are also points of vulnerability where government agencies could find themselves out of compliance with their nation's information privacy and security requirements. Citizens' legally protectable information is at risk every time a service—or benefit-related document containing it is created, scanned, copied, printed, faxed or emailed.

Nuance adds a layer of security and control to government's paper-based and electronic processes, enabling secure use and exchange of protectable information. This advanced capture and output platform helps government agencies improve efficiency, reduce error, assure compliance and mitigate the other risks and costs of security violations and privacy breaches.

For every 100 Internet users in Europe, approximately 56 personal information records have been compromised through various forms of data breach.

Government executives' top concern: Security

Even as governments need to make information easier to access, work with and share, they need to keep it secure. This challenge comes at a time when the frequency and costs of data breaches are on the rise.

In its April 2014 report, Information Security: Federal Agencies Need to Enhance Responses to Data Breaches, the U.S. Government Accountability Office reported that the number of information security incidents in federal agencies had doubled between 2009 and 2013, to 25,566 per year. While comparable figures are not available for Europe (for example, the annual Breach Level Index from data security firm Gemalto reported 190 breaches in Europe and only 1,541 worldwide) the trend is the same: increasing. A study by the Central European University's Center for Media, Data and Society (CMDS) says that for every 100 Internet users in Europe, approximately 56 personal information records have been compromised through various forms of data breach.

Ponemon Institute's 2015 Cost of Data Breach Study: Global Analysis placed the worldwide average total cost of a data breach in 2014 at $3.79 million, a 23% increase over the prior year. Data breaches were costly everywhere, averaging $6.5 million in the United States, £2.37 million in the United Kingdom, €3.52 million in Germany and €3.12 million in France. In the public sector, the average cost per stolen record was estimated at $73.

$6.5M

The average cost of data breaches in the United States in 2014

Of course, all of these industrialized nations have stringent data privacy laws mandating the protection of personal information and imposing penalties when it's exposed. Government agencies themselves can be subject to the requirements of laws such as the Data Protection Acts in France and the UK, the Federal Data Protection Act (Bundesdatenschutzgesetz) (BDSG) in Germany, and the Health Insurance Portability and Accountability Act (HIPAA) and Gramm-Leach-Bliley Act in the U.S. States in both Germany and the U.S. have their own privacy laws.

And the rules continue to change. Germany enacted legislation in July 2015 ordering over 2,000 essential services providers to implement new minimum standards for data protection within two years or face fines up to €100,000. If keeping up with changing regulatory requirements weren't difficult enough, the compliance challenge for government agencies is that the threats to their information come from all directions.

For starters, paper is inherently insecure. This was demonstrated in the exposure of names, Social Security numbers, addresses, phone numbers, and other information on 3,000 residents of Warren County, Iowa, when paper records from the Iowa Department of Human Services were not shredded as intended following a fire that destroyed the agency's offices. Instead, a county maintenance worker mistakenly returned a container of damaged records from temporary storage back to the destroyed building. The mistake was only discovered when DHS received a call from a nearby resident who had found a DHS document in her yard.

In some ways, it increases it. Malicious or criminal attack on computer systems remained the leading source of large data breaches worldwide in 2014 (at 47%), but more than half stemmed from causes under the victimized organization's control: 25% of breaches involved human error, such as mistakes or lapses leading to theft or loss of portable devices such as laptops, tablets, smart phones and USB drives containing individuals' personal information; 29 percent resulted from IT system glitches or business process failures. Throughout Europe, according to the CMDS study, the main cause of privacy breaches was an organization's own errors, insider abuse and other internal mismanagement.

25%

of breaches involved human error, such as mistakes or lapses leading to theft or loss of portable devices such as laptops, tablets, smart phones and USB drives containing individuals' personal information.

One of the most serious cases of employee error comes from the UK, where personal data on every family claiming universal child benefits—including names, addressees, national insurance numbers and bank account details — was reported lost when two password-protected CDs sent through the mail by a worker at Her Majesty's Revenue and Customs (HMRC) never arrived at their destination. The breach affected 25 million people, over 40% of the nation's population. The chairman of HMRC resigned when the breach came to light.

Also in the UK, after a non-secure hard drive containing intelligence information on approximately 16,000 prisoners disappeared from a prison office, the prison service distributed new encrypted hard drives to 75 prisons throughout England and Wales still backing up data to devices lacking encryption or password protection. When another hard drive—this one containing information on 2,935 prisoners—subsequently turned up missing from another prison in the same way, an investigation by the Information Commissioner's Office (ICO) revealed that the prison service had not realized that the encryption capability required activation. ICO fined the Ministry of Justice £180,000 over the incidents.

An employee of the Australian Department of Immigration and Border Protection mistakenly e-mailed to organizers of the Asian Cup soccer tournament the dates of birth, passport numbers and other personal details of 31 world leaders just a few days before their arrival for the 2014 G-20 summit in Brisbane. The agency did not report the breach to the affected world leaders, even though laws in some of their nations, including the UK, France and Germany, require notification of any victims of a data breach.

Unfortunately, internal security vulnerabilities and potential compliance breaches exist at every information touch point.

Unfortunately, internal security vulnerabilities and potential compliance breaches exist at every information touch point.

Mobile phones and tablets, whether agency—or employee-owned, can be lost, stolen, or used inappropriately in the workplace. In the U.S., Nurses at a Wisconsin hospital were fired after posting cell phone pictures of a sensitive and potentially embarrassing patient X-ray on Facebook. Three Connecticut hospital employees were fired and four others disciplined after a clinician posted cell phone photos of a dead teenager's gunshot wounds.

Analog fax machines lack controls or activity logging, making it too easy to send faxes to wrong numbers and have that error go undetected. Unsecured digital MFDs can be used to make unauthorized copies or scans. In the absence of automated encryption and file destination control, citizen information can be accidentally or intentionally emailed from these devices to unauthorized addresses. Printing of social service-related documents to shared MFDs risks exposure of sensitive information in papers left sitting in the output tray or picked up by the wrong person. Documents stored in the MFD's hard drive could be improperly printed out or copied onto a USB stick. Email addresses, network and user IDs and even passwords stored in the device's memory can be accessed by someone with the right skills.

If government CIOs aren't fully aware of these risks, government legislators and regulators certainly are.

The U.S. Federal Trade Commission (FTC) puts it plainly: "Digital copiers are computers." Its report, *Copier Data Security: A Guide for Businesses*, goes on to recommend that organizations incorporate these devices into their information security plans. Likewise, a security risk assessment tool prepared by The Office of the National Coordinator for Health Information Technology mentions copiers 15 times as being workstations on which Protected Health Information must be secured with administrative, physical and technical safeguards.

The only way to protect data at rest, data in motion and data in use is with a system that combines enforced but unobtrusive user authentication and authorization with automated encryption, destination and output controls and audit trails. That's how the modern government agency assures the integrity of citizen information wherever paper is required and on whatever device information is accessed or transmitted.

The only way to protect data at rest, data in motion and data in use is with a system that combines enforced but unobtrusive user authentication and authorization with automated encryption, destination and output controls and audit trails.

Government's challenge: Do new with less

Governments around the world generate and depend on more content, data and paper than any other industry. Whether in legal case management, freedom of information response, grant administration, benefits claims processing or immigration review, government processes are inherently paper-intensive experiences. And paper is inefficient, costly and unsecure.

It's past time to break free of paper

In one recent study, two-thirds of U.S. state and local government agencies reported they spend more than one-third of their time processing paper documents. It's no surprise. In a global survey of 1500 owners of document-driven processes, IDC found paper documents, rather than electronic information, to be the driver in 58% of government constituent-facing processes and 46% of internal or back-office processes. As extensively as government relies on paper, barely 36% of government respondents described these processes as efficient and effective.

Government certainly knows that automation could increase efficiency, reduce costs and improve quality of constituent service. The U.S. Paperwork Reduction Act of 1980 and the European Commission's 2005 decree on document management established foundations for process improvements years ago. IDC found that governments could reduce operating costs over 9% by optimizing document processes. But they also found only 33% of government respondents place great importance on fixing their document-driven processes.

This could be on the verge of changing. In the Association for Information and Image Management (AIIM) Paper Wars 2014 survey, 68% of respondents across all industries agreed that business-at-the-speed-of-paper will soon be unacceptable. Citizens who have grown accustomed to the increasing ease and efficiency in their dealings with private sector enterprises may come to expect their engagement with government also to be as close and convenient as their personal computer or mobile device. Government agencies and departments will need to transition from "we have a form for that" to "we have an app for that."

At the same time, Gartner says that from the front lines to the highest level executives, the government workforce of the future will be more digitally literate than ever. This younger generation of knowledge workers will come to their jobs expecting to find modern collaborative technologies for creating, sharing and applying information.

Some of those enabling technologies are, of course, already in place, but governments may not be putting them to best use. Government agencies everywhere have data networks that connect their workers with each other and the information needed to do their jobs. And they have fleets of multifunction devices (MFDs) that not only copy and print but can scan documents into document management systems (DMS) or transmit them by email or fax. But there's no way for these devices to improve efficiency if they can't connect directly to the document collaboration systems in an intelligent way—or if workers don't know the best practices for using them. For example, AIIM reported that 35% of scanned documents are born digital: created on computer, printed out, then unchanged when they go to the scanner. Another 16% of scanned documents are photocopied before scanning, and 65% are not destroyed after scanning.

65%

of documents are not destroyed after scanning.

Government could reduce inefficiencies such as these by automating the manually intensive processes of getting information off of paper or out of email, into a DMS or business process, and then routed in digital form automatically to the correct folders, the workers who need them or other appropriate destinations.

Automating government document processes for efficiency and security

Nuance provides government agencies worldwide with a comprehensive platform for streamlining and securely managing document-related workflows, including distributed document scanning, mobile and electronic capture, and print management. Integrating mature Commercial Off-The-Shelf (COTS) products into a single integrated package, Nuance enables agencies to eliminate the drag and exposure of paper, with an automated solution that increases efficiency, reduces costs and improves compliance. Nuance adds a layer of security and control to electronic information and the output of documents, assuring the integrity of citizens' personal information wherever paper is required and on whatever device information is accessed or transmitted.

Securing information at every touch point

The Nuance solution effectively and transparently enables essential best practices for the secure and compliant handling of personal information created, copied, output or shared on smart devices—MFDs, mobile phones, tablets, and laptops.

– **Require user authentication**
Security begins by controlling access to the control panel. Nuance requires users to verify their credentials at the device, by PIN/PIC code, proximity (ID), or by swiping a smartcard to access documents containing protected information. This capability helps U.S. agencies comply with Homeland Security Presidential Directive 12 (HSPD-12) that requires authentication with government-issued CAC or PIV cards, and allows government departments anywhere to restrict access by two-factor authentication.

– **Restrict access based on user authorization**
Once users are authenticated, the solution applies rules and permissions to control what they can do on the MFD. Single sign-on network authentication is seamlessly integrated with document workflow, to ensure optimal security.

– **Centrally audit all network activity**
Nuance centrally captures and stores a complete audit trail of all MFD and document activity, so that in the event of a data breach, you can easily identify which device was the source, who was the authenticated user and where the data was sent. Nuance also records all metadata passed through the system, enabling you to track any specific scan, print, copy or fax to a specific user or produce reports providing an overview of selected activities by device or department.

– **Encrypt data to and from MFDs**
Leveraging accredited methods for both Data in Motion and Data at Rest, Nuance encrypts communications between smart MFDs and mobile terminals, the server and allowed destinations, to ensure documents are only visible to users with proper authorization. This includes Secure Sockets Layer (SSL) with up to 2048-bit encryption and FIPS 140-2 accredited Open SSL FIPS Object Modules on supported MFDs.

– **Only release print jobs to authorized personnel**
When documents need to be printed, Nuance prevents exposure of citizens' personal information by holding print jobs in a secure print queue and not outputting them until the employee signs in at the printer and selects the specific documents to output.

– **Implement rules-based printing**
Nuance's print management platform allows agencies to build, implement, and automatically enforce new or existing print policy rules to control print activity. Rules can define who may print which types of documents, when they may output them, and where they can print. Administrators can restrict printing based on user or group membership, source application, time of day, and destination. Rules can also be defined based on the content of the print jobs.

– **Enforce trusted network destinations**
Nuance validates the information in scanned documents to automatically prevent their transmission to unauthorized fax numbers, email addresses or even domains. For the most granular control, allowable destinations can be part of a specific user's pre-defined workflows, so they may only send documents to the recipients in an approved list displayed in the control panel.

– **Monitor and control personal information activity**
Nuance provides a centralized approach to protecting personal information with advanced content filtering that can examine and intercept documents that contain security classification keywords or sensitive data such as account or case numbers. Documents containing content that should not leave the agency can be quarantined or deleted, with the user and security officer automatically notified of that action.

– **Standardize and integrate network scanning**
One common problem with traditionally configured office MFDs is that no two devices within an organization are setup the same way for document scanning. Nuance eliminates this shortcoming and simplifies workflows, by standardizing the scanning process across an entire fleet of MFDs. With integrations enabling direct scanning into all major document systems, Nuance provides more security than scanning into network folders.

Nuance's print management platform allows agencies to build, implement, and automatically enforce new or existing print policy rules to control print activity. Rules can define who may print which types of documents, when they may output them, and where they can print.

Simple, streamlined processes in action

Some everyday activities—the processing of an application for government benefits or a freedom of information (FOI) request—illustrate the speed, efficiency, security and economy of the Nuance-enabled document workflow.

– **Digitizing documents at the point of origin**
In one example, a citizen seeking some type of public benefit comes to the local office of a government agency with all of the materials needed to support her application, including photo ID, proof of residence, financial information, and more. An employee initiates the application process, either reviewing the applicant's manually completed form or entering information into her computer to create an electronic form.

To build a complete electronic application package, the employee will use the office's MFD to scan all of the citizen's documents instantly and directly into the agency's application processing system. To unlock the MFD, she authenticates herself by swiping a proximity ID card or entering her username and password or PIN number on the machine's front panel or on a mobile device. With the worker securely logged in, the MFD touch screen displays buttons for the functions or pre-defined workflows she's authorized to use. In this case, one of these workflows will scan the documents and route them directly to the team in another location that reviews and approves applications. Within seconds, she'll receive an automated notification confirming the successful scan, including the total number and type of pages.

Everything about Nuance's automated processes is designed to simplify use, minimize user tasks and reduce risk.

– **Automating error-prone manual tasks**
Everything about Nuance's automated processes is designed to simplify use, minimize user tasks and reduce risk.

Imagine an FOI officer at an environmental regulatory agency who has a statutory deadline for responding to a reporter's written request for copies of all correspondence on a recently decided matter. His authorized FOI workflow allows him to scan the request at an MFD, assign a case number and barcode, and route it to offices where relevant documents might reside.

Scanning of the located documents is fully automated, transforming data into standard formats without the user needing to know or specify any input or output settings. Also automated are routine, error-prone tasks such as batching, splitting, filing and indexing of scanned documents. Validation and filtering at the point of origin ensure accurate document handling and routing, including the immediate routing of documents requiring wet signatures.

In both the benefit application and FOI scenarios, fully automated data extraction, document type identification (with or without barcode), document de-skewing and cleanup, blank page removal and double-sided scanning speed the handling and processing of documents, increase accuracy of the assembled packages and eliminate the delay and errors of manual rekeying.

After the requested FOI documents are securely captured, extracted and classified, the Nuance solution automatically converts them into full text searchable digital PDF files and securely routes them for further review. Documents can be redacted both when scanned and when printed.

In the benefits workflow, for example, bi-directional database look-up can auto-fill fields for faster completion of applications from citizens who may have already received services from the same agency. For any process, entire workflows can be pre-defined and saved to a single button, but when additional user action is required, visual prompts make that clear and limit human error.

– **Accepting documents from any input source**
Nuance captures documents from any input source, including scanner, email, fax, Web forms, and mobile devices. So in whatever form the information exists, it can become part of the citizen's application file.

Tablets and laptops can free workers from the office, enabling them to go to the constituent to provide more personalized and efficient service. Voice recognition for speaking information into a mobile electronic form can be faster and more accurate than manual keying on a small device's touch screen. Nuance enables the use of smart phone and tablet cameras in place of scanners to capture paper documents and add them to the workflow. Since data entry or image capture happen directly within the Nuance mobile solution, with nothing stored in the device, there is little risk of information being compromised if the device is lost or stolen.

Nuance captures documents from any input source, including scanner, email, fax, Web forms, and mobile devices.

Delivering measurable results for government agencies worldwide

The operating improvements that can be achieved with Nuance technology are not merely possible, but are already being realized by agencies at all levels of government every day.

For Telford & Wrekin Council, a 166,600 population borough in the West Midlands region of the UK, a Nuance networked print management solution helped the local government streamline administration functions and reduce paper waste, contributing to estimated cost savings of 25 percent over four years. The Nuance solution enabled Telford & Wrekin to consolidate hundreds of standalone desktop printers, copiers, scanners and fax machines down to 66 color and black and white MFDs running Nuance software with integrated print management, job tracking and user mobility, plus a smaller number of specialized devices.

Some of the Council's most immediate improvements came from implementing pull printing that allows employees to walk up to any MFD on the network, authenticate themselves, and print out their queued documents. This capability supports worker mobility, eliminates wasteful unclaimed printing, and increases security, since documents are not output until the user is physically at the machine to retrieve them.

For the U.S. Citizenship and Immigration Services (USCIS), a Nuance automated document capture and distribution solution reduced the time for field offices to prepare and submit N-400 Application for Naturalization forms to one of the agency's service centers by 50 to 65 percent. Lack of automation in the application preparation process had stretched the average cycle time 5.1 months, with a backlog of some 300,000 cases. Conversion of paper documents to PDFs had become a nine-step process:

1. Receipt of a bundle of N-400 applications at field office/intake center
2. Bundle disassembled, N-400 forms removed
3. Applications scanned one at a time on a networked MFD
4. Scanned documents transmitted to a USCIS email address
5. Worker elsewhere in the field office opens the email and saves the attachment as a PDF in a folder on the network
6. File is renamed from the default scanner-assigned name to Axxx.pdf
7. Compression and encryption of each application using a desktop tool
8. Emailed of applications to the service center; but because of email attachment size limitations, no more than 5 applications can be attached to any email
9. A separate email is sent providing the password to enable the encrypted files to be opened at the service center.

The Nuance solution replaced this inefficiency with a four-step highly automated process:

1. Bundle of N-400 applications received at field office
2. Bundle prepped for scanning with barcode sheets
3. Entire batch scanned on networked MFD, with user invoking a secure workflow at the push of a single button
4. Nuance software handles the rest, automating tasks that were formerly performed or initiated by hand:
   - FIPS 140-2 encryption at the point of scan
   - Batch splitting into individual applications
   - File renaming and conversion to text-searchable PDF
   - Storage in a secure file location for agency access
   - Email sent notifying agency that files are available

The streamlined process helped to reduce the number of pending cases by up to 50%.

Differences that matter

Nuance has years of experience serving government agencies and the industries they regulate. Our government document capture workflow and print management solution reflects both our industry-specific experience and exclusive focus on the vulnerabilities and compliance exposures of paper processes. That's also why we offer a complete solution enabling government agencies to securely capture and distribute information—not only at point of origin but anywhere in their decision-making process that documents must be accessed, output and shared.

To help governments contain IT costs, Nuance supports the largest number of hardware devices and backend systems in the industry. Integrating with existing software and systems, the Nuance solution simplifies deployment and helps agencies leverage their existing technology investments. By adding comprehensive print management to a document capture and workflow solution, organizations can consolidate printer fleets and reduce overhead.

In addition to its cost-saving benefits, Nuance-enabled rules-based printing is also an effective green initiative, allowing an organization to set up the print rules necessary to reduce paper waste and conserve printer materials at all levels, from energy consumption to ink usage. In fact, Network World Magazine named the Nuance platform one of the Top 12 Green IT products in the "Going Paperless" category, identifying it as one of the best environmentally friendly solutions for reducing an organization's reliance on paper.

With its extreme ease of use, non-disruptive operation and transparent security and control, Nuance enjoys industry-leading rates of user adoption and satisfaction.

Conclusion

Demographic and economic forces are driving governments to change how they create, share and apply information. Citizens want to engage their governments in more modern ways, confident their personal information will be protected. A digitally literate workforce wants to respond, but tight budgets are a persistent challenge. So documents remain a leading source of expense, inefficiency and risk.

Nuance replaces governments' costly and non-compliant paper-based document processes with electronic document capture and distribution solutions that place smart devices at the center of efficient and secure automated workflows. Nuance provides the control that minimizes risk and assures compliance, while at same time streamlining processes and reducing costs.

Nuance provides the control that minimizes risk and assures compliance, while at same time streamlining processes and reducing costs.

To learn more, visit www.nuance.com/imaging or call 800-327-0183.

About Nuance Communications, Inc.
Nuance Communications is reinventing the relationship between people and technology. Through its voice and language offerings, the company is creating a more human conversation with the many systems, devices, electronics, apps and services around us. Every day, millions of people and thousands of businesses experience Nuance through intelligent systems that can listen, understand, learn and adapt to your life and your work. For more information, please visit nuance.com.

NDI–94 DEC 2015