



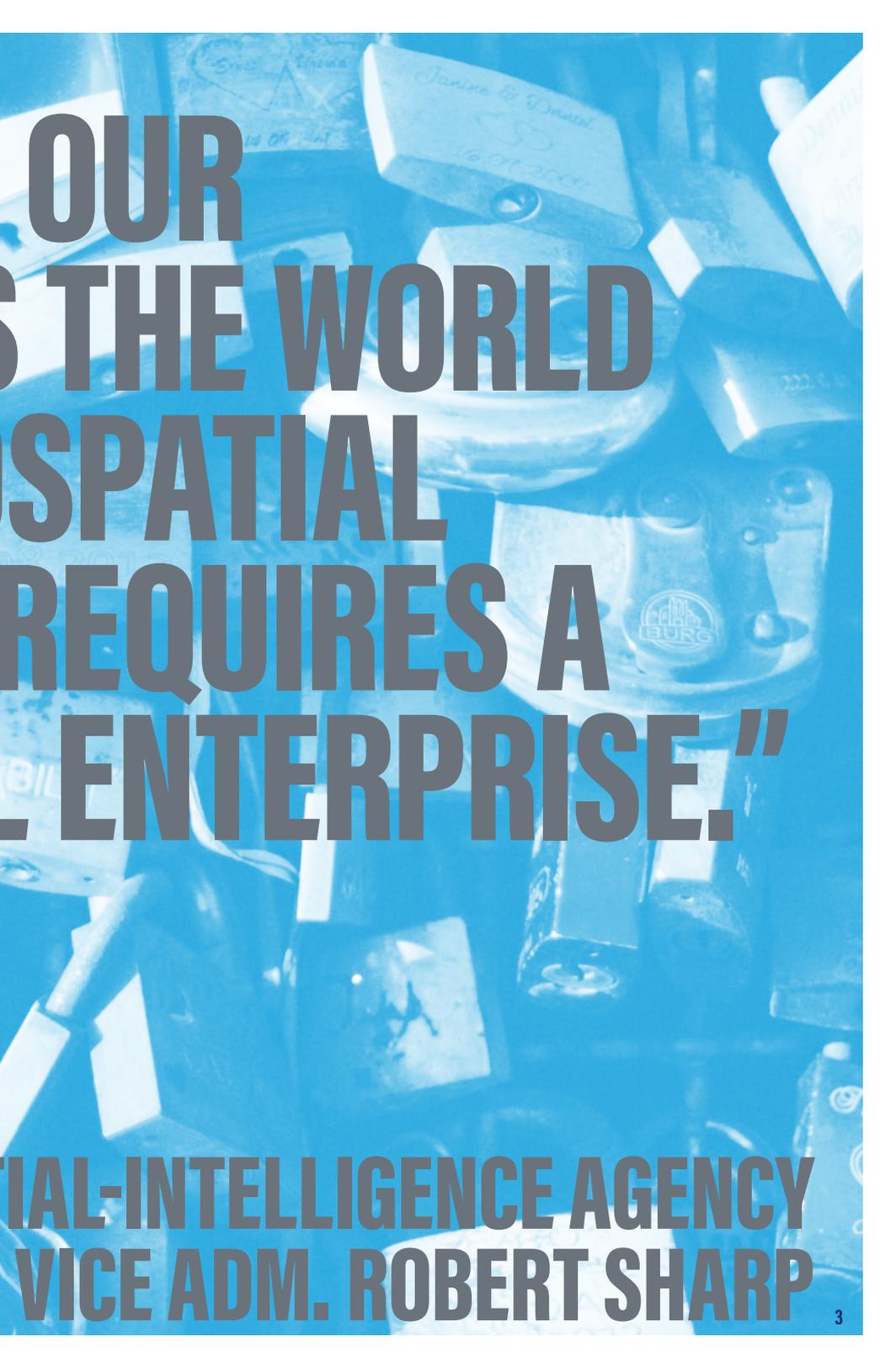
**IMPROVING DIGITAL  
EXPERIENCE IN THE  
NATIONAL SECURITY  
COMMUNITY:  
BREAKING DOWN  
WHAT YOU NEED  
TO KNOW**

**GOVLOOP  
POCKET GUIDE  
2020**



**“MAINTAINING  
ADVANTAGE AS  
LEADER IN GEO  
INTELLIGENCE  
SOUND DIGITAL**

**- NATIONAL GEOSPATIAL  
DIRECTOR**



**OUR  
S THE WORLD  
SPATIAL  
REQUIRES A  
ENTERPRISE.”**

**IAL-INTELLIGENCE AGENCY  
VICE ADM. ROBERT SHARP**

# CONTENTS

Executive  
Summary

**05**

The Business  
Experience  
Wave In  
National  
Security

**06**

Organizations  
Look to  
Content to  
Help Deliver  
Compelling  
Experiences

**08**

Zero Trust  
Content  
Security

**15**

How to Start  
Increasing  
Content  
Velocity,  
Security and  
Intelligence

**20**

Reimagine  
Your Digital  
Experience

**24**

Cheat Sheet

**30**

Conclusion

**31**

# EXECUTIVE SUMMARY

Information technology that supports interoperability, breaks down silos and enables the secure sharing of information is crucial for the Intelligence Community (IC), Law Enforcement, Public Safety and other national security mission partners. Too often, outdated technologies and policies create cumbersome workflows that hinder daily business processes. To meet their missions, agencies need a cohesive information ecosystem built on open standards that enables them to collect, manage and share digital content efficiently and securely. That ecosystem sets a foundation for creating frictionless business processes and collaborative communications, opening endless opportunities for collaboration across an organization.

Unfortunately, a mix of technologies that serve limited purposes is a challenge for the National Security Community. Complications result because what works for one agency may not work for another. To manage a vast amount of data, people and processes, the National Security Community has thousands of operational systems and networks, which can make for a siloed workforce, in turn, data and content out of context.

In thinking about these challenges, keep in mind the difference between content and assets. Digital content is any type of data that can be stored and managed. An asset presents content as a digital document, image, video or audio that can be managed and protected as a self-contained, unique unit. To create an information ecosystem, agencies need to ensure they can securely share both content and assets.

To overcome those challenges, many are looking for ways to harness technology to improve digital experiences, and better deliver critical information to the workforce. Agencies are encouraged to use approved digital tools and capabilities to the greatest extent possible. Accessibility standards, increased data-sharing initiatives, commercial technology advancements, and user expectations are driving factors in the paradigm shift to free the data while protecting the information.

Furthermore, from policy mandates to rising workforce expectations, to working from home overnight, several key factors are making change inevitable in the National Security Community:

- Endless “opportunities” for organizational integration
- Maintaining mission-readiness in a constantly changing environment
- Protecting information to share
- Enabling a unified, agile, and trusted workforce

GovLoop partnered with Adobe, a digital service provider, to produce this Pocket Guide and share how the national security community is improving the digital experience in three areas:

- Accelerating content creation to enable the mission
- Creating a user-centric data experience
- Shifting toward a zero-trust architecture

To do this, we'll look at how the IC security environment has evolved and what's required for effective and secure collaboration today. Plus, we'll hear expert tips about how the IC community can redefine its digital experiences.

# THE BUSINESS EXPERIENCE WAVE IN NATIONAL SECURITY

The global technology changes and adoption of cybersecurity, cloud, artificial intelligence and machine learning, as well as information and asymmetric warfare by our adversaries have put pressure on IC, Law Enforcement, Homeland Security and Public Safety to quickly deliver accurate and timely content at scale is greater than ever. The National Security Community requires secure, agile IT infrastructures that interoperate seamlessly across security fabrics and leverage industry's innovation and speed – all the way to the mission edge. With volumes and variety of data, the workforce desires the same digital experience they have at home and outside the office. The IC, Law Enforcement, Homeland

Security and Public Safety have experienced waves of disruption and transformation before.

The first wave of enterprise disruption affected the back office and began in the '60s, in the early days of computing. During this period of early computing and networking, it became possible to digitally connect different parts of an organization. Imagine how slow, inefficient and error-prone these processes were with people writing things down on paper, walking to the building next door and filing something in someone else's to-do box.

When organizations realized that they could digitally connect their backend systems, they

were astounded at how much productivity and efficiency they could achieve. The strategy discussions were about how they needed to adopt these systems and capitalize on Enterprise Resource Planning (ERP). This was the “back-office” wave of transformation. The ERP product, which was once considered a bold and even risky investment, is now part of the enterprise infrastructure for most organizations. But they no longer offer the efficiencies they once did — it’s table stakes.

Shortly after the back-office wave came the Customer Relationship Management (CRM) revolution that focused on transforming the “front office,” managing the workforce, citizens and other customer interactions. These CRM systems empowered firms to keep track of customers and selling conversations, share that information with their teams, and more efficiently manage their sales processes. Once again, the strategy discussions were about productivity and cost savings. But today, CRM products are ubiquitous, and this has caused organization efficiencies to recede. It, too, has become table stakes.

As part of the second wave, in 2003, Adobe pioneered Content Security (Digital Rights Management - DRM) for protecting university transcripts and documents from being tampered. In 2007, Adobe transitioned to a subscription-

based business model, allowing content creators to design and innovate faster through the cloud while continuing to support on-premises environments to enable disconnect or edge operations. In 2013, the Intelligence Community awarded Commercial Cloud Services (C2S) to advance Cloud Computing in their fabrics. In 2018, Microsoft agreed to do the same and migrate on-premises software to Microsoft Office 365 and Azure Cloud Services.

Now, we are at the beginning of the third wave of enterprise transformation. This wave also spawns from new technology, but that’s where the similarities end. The previous two waves were about the business processes. This wave is about modernizing the business experience organizations provide to people around content. This wave is about **Content Velocity, Security and Intelligence**, while providing the ability to **Create Once, Publish Everywhere**. These are just a few of the folks who contribute to making well-informed decisions as efficiently as possible, wherever they are working.

We call them Content Creators. As you can see, Content Creators are NOT just those who went to media, marketing, art or design schools. All of the people within an organization — from top management to the receptionist — are Content Creators.





**ORGANIZATIONS  
LOOK TO  
CONTENT TO  
HELP DELIVER  
COMPELLING  
EXPERIENCES**

Today, Content Velocity is more important than ever, but many organizations still struggle. All too often, organizations are unable to build enough content to keep pace with business or mission demand. Users and Content Creators are unable to find and repurpose the right content, for the right context, at the right time. With the IC, organizations must make content and data easily discoverable and sharable across the community while balancing the protection of that content.

For example, research shows that depending on the type of content and finished product, it might still take almost two weeks to create and deliver one piece of content. That might not seem like too heavy of a lift, but when you factor in the growing expectation of peoples' experiences and mission urgency, two weeks can be an eternity to get content to the relevant audiences. Imagine there is a crisis, event or mission that your team needs to address, but the mission will be relevant only for three or four days. If it takes almost two weeks to get relevant content to market or specific stakeholders, you've already missed the opportunity to capitalize on that moment. Content Velocity problems can be grouped into seven different buckets:

- Resource constraints, limited expertise, and siloed departments that make it hard to effectively deliver content experiences based on data.
- Slow time from creation to delivery of new digital assets and experiences, including time to deploy content and make changes.
- High cost and complexity of stitching together disparate digital asset management systems, tools and workflows.
- Inefficient content controls, creation and signing processes that bottleneck publishing to the web and other channels.
- Inability to track experience impact because your organization does not have the data necessary to gauge content performance.
- Need to comply with directives, regulatory mandates and auditability standards.
- Transitioning from traditional perimeter-style defenses with multiple network zones, firewalls and encryption to adopting a Zero Trust posture.

Addressing these problems lies at the heart of the **Content Velocity** use case. The synergy between Creative Cloud applications and Adobe Experience Manager Sites, Assets, Forms, and Adobe Analytics empowers leading brands and public sector organizations to transform their experience management architecture. It transforms from a messy knot of disconnected point solutions to a solution built on open standards that leverages intelligent automation to create, manage and deliver experiences across every touchpoint, screen size and device. Supporting our solutions is Adobe Sensei, which uses artificial intelligence and machine learning to power intelligent features that dramatically improve your digital experiences.

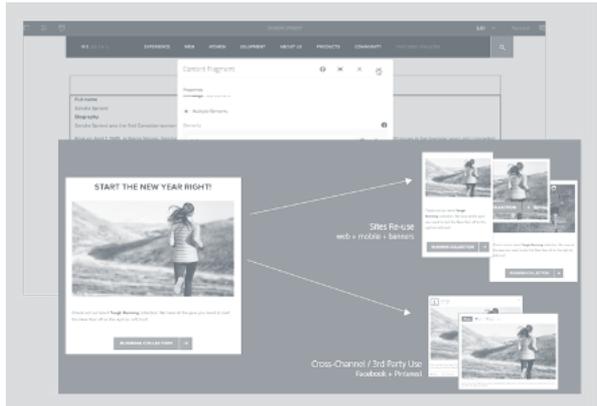
One of the quickest ways to generate content velocity is to ensure all Content Creators, publishing stakeholders, and users have access to the assets they need. Ensure they can quickly find the assets they need, and easily find assets to re-use so they can be confident that they are using the most current, approved versions of the content they are publishing. Asset management, powered by AEM Assets, is the backbone of the Content Velocity use case. AEM Assets provide an enterprise-grade repository that streamlines asset search, eliminates dark assets that can't be found, and supercharges asset re-use to increase return on investment. AEM Assets form the bedrock of the dynamic content engine that forms the Content Velocity use case. A Forrester and Gartner leader, AEM, is used extensively in both the commercial and public sectors and is authorized at [FedRAMP Moderate](#) and Department of Defense [Cloud Computing System Requirements Guide Impact Level 4](#) (SRG IL4).

# CREATE ONCE, PUBLISH EVERYWHERE

Not only does the Content Velocity use case streamline upstream creative and publishing workflows, but it can also automate downstream experience delivery workflows using industry-leading capabilities. AEM Assets can leverage one master file to auto-generate and publish unlimited versions, changing size, format, resolution, crop, or effect. It eliminates the need to pre-create and pre-store countless versions of the same asset for delivery across different screen sizes and devices. By automating this process, Content Creators dramatically reduce the size (and cost) of their Digital Asset Management (DAM) repository. Automation also ensures Content Creators provide a consistent, quality experience, regardless of what device or channel they deliver to; they can always deliver the right size asset to the right sized experience.

Full-sized video is also auto-sized for all screens and adaptively streamed, meaning the file size is reduced on the fly when bandwidth falls; ensuring a smooth, uninterrupted viewing experience regardless of connection speed. Assets can also optimize other manuals, tedious workflows required to deliver experiences across devices. There are capabilities like Smart Crop for image and video, which leverages Adobe to automatically detect the focal point of an image or video, and crop to that focal point across an unlimited amount of aspect ratios. By automatically delivering the right sized asset to every experience, and by automating previously manual asset optimization processes, AEM Assets dramatically cut the time it takes to optimize experiences for delivery across channels, providing yet another source of increased Content Velocity.





**Modular Experiences.** The above capabilities can be supercharged when we add in AEM Sites, which gives organizations the ability to scale the automation of device-optimized experiences even wider. Customers using Sites and Assets can easily provide website authors with a comprehensive view of the breadth of their organization's digital content, and easily add interactivity and rich video elements. However, the greatest synergy between Sites and Assets lies in the power of Experience Fragments, which ensure websites, ads, and other digital experiences look great by leveraging modular templates.

Instead of creating one standalone experience in multiple segment-specific variations, which can be very time consuming and can constrain personalization efforts, Experience Fragments allow authors to leverage an experience template. Each area of the experience template can be automatically populated with the content that will most resonate with its customer segment. Experience Fragments empower website authors to create the logic around a single experience template and completely automates the population of that template based on the delivery segment. It dramatically reduces the time needed to scale experiences across segments, increasing the speed of experience delivery.

Beside organizations external websites, knowing where and how the workforce consumes, shares and make decisions based on content is crucial to establishing an effective and efficient communications strategy. Adobe uses AEM to produce Inside Adobe, its 20,000+ employee worldwide intranet. Inside Adobe was named to the Nielsen Norman Group yearly list of "10 Best Intranets." Citrix, Walmart and UBS also use AEM for their global employee intranets, allowing them to deliver engaging experiences.

Previously, Adobe used a decentralized publishing model, with each department managing its own site. But the Digital Communications department wanted to standardize Inside Adobe and deliver targeted content to each employee. With AEM, every Adobe department can publish content and edit its own intranet pages without having to involve IT. Departments use templates and best practices developed by the Digital Communications team. Departments can also save time and maintain consistency by using shared assets via the AEM Assets capability. So far, the Digital Communications team has moved 60 department sites to a single instance. Digital Communications also measures employee engagement through Content Intelligence. The improvements to Inside Adobe increased employee satisfaction from 75% to 94%.



Visual Specialist



App Test



Public Affairs



Analyst



Reviewer

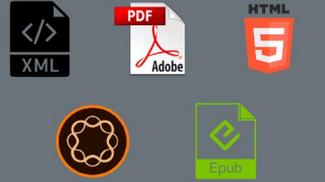


Trainer

CONTENT

Technical Documentation  
 Analysis Reports  
 RFx/Proposals  
 Help Documentation  
 Knowledge Base  
 API/Code  
 eLearning Content/Guides

Step-by-step Walkthroughs  
 User Guides/Release Notes  
 Legal Compliance  
 Maintenance  
 Requirements/SOWs  
 General Reports  
 SOPs/CONOPs



OUTPUT



Designer



Tech Doc Spec



SME



UI/UX



Copy Editor



Legal

**Content Authoring.** Especially within the Intelligence Community, Law Enforcement, Homeland Security, and Public Safety missions, the velocity of authoring and publishing reports matters XML Documentation Add-on to AEM Assets provides Content Creators a unified platform create, collaborate, edit, and publish reports and documentation in multiple formats (AEM Sites, responsive HTML5, mobile apps, PDF files, EPUB files, Kindle file format, and more) and at multiple classification levels from a single source. Because AEM is so flexible, the team can create any kind of site structure and navigation they want and explore new content strategies. Organizations can deliver content in new formats as needed to provide customers with the best possible customer experience.

Content Creators can author from anywhere using the user-friendly web-based DITA editor, or they can choose from multiple authoring modes that make it easy for subject matter experts or casual contributors to author DITA content without XML programming skills. If they have legacy content created in Word, XHTML, InDesign and unstructured FrameMaker content, it can be easily converted to DITA in seconds with out-of-the-box automated conversion support. Consistency and reuse may also be very important to the design philosophy for many organizations. Templates in Assets allows the teams to maintain a consistent design and deliver on expected finished quality.

# IT'S NOT ABOUT THE FORM... IT'S ABOUT VELOCITY OF ITS CONTENT (DATA)

Given organizations' previous emphasis on streamlining "back office" operations and business management, many are now realizing that their operational processes start and end with a static, paper-based form online in Portable Document Format (PDF). While organizations have started their transformation to meet digital-first, or in some cases digital-only, environment, legacy paper-based or manual steps often interrupt developing digital processes, such as posting a simple PDF form online that then requires printing, signing, and mailing, scanning, or waiting for information to be entered into an IT system. Transformation may be complicated if an organization uses HTML5 or XML Forms, but also has created an archival PDF of the content to be compliant with the National Archives and Records Administration ([NARA](#)) mandates or IC policy. With government continuity and operational success facing its greatest test in our modern era, as well as increased data-sharing initiatives, the need to "free the data" — by streamlining and accelerating simple content, documents, and forms processes, and signing them — has never been greater.

Some organizations try to answer this challenge by building tools in-house to meet rising customer expectations. Yet, these solutions are often expensive, difficult to scale across the hundreds of

forms, and highly reliant on limited IT resources, especially in a telework environment. AEM Forms technology offer increased performance, improved data usability, greater efficiency, enhanced workflows, and security for sensitive data collected via forms. The Adobe digital forms maturity model shown above offers a tailorable methodology to enhance agency form capabilities, starting with basic paper-based form processing and evolving to dynamic forms that incorporate machine learning and artificial intelligence. Adobe understands that adapting forms is an evolutionary process and is dependent on factors like available technology, skill sets and budget.

Built on an open architecture platform, HTML and PDF forms are built with a seamless, engaging user experience to create, manage, publish and update complex digital forms while integrating with back-end processes, business rules and data. With the authority to operate on-premises or in a secure cloud environment, Forms can be integrated with processes to reduce errors, paper use and time spent on content and data collection. At the same time, efficiency and user experience improve. Third-party solutions like ServiceNow, Microsoft Dynamics, Salesforce and SAP can also work with Forms. Agencies can deliver content for different languages, regions and customer segments while helping to meet Section 508 accessibility standards for any device.



**Automated Forms Conversion.** Wouldn't it be great to transform batches of static forms into a mobile responsive, optimized form-filling experience without the laborious work and high cost? Automated Forms Conversion is a cloud-based micro-service that helps accelerate digitization and modernization of data capture experience through the automated conversion of PDF forms to adaptive forms. The service, powered by Adobe Sensei, automatically converts your PDF forms to device-friendly, responsive and HTML5-based adaptive forms. While leveraging the existing investments in PDF Forms and XML Forms Architecture (XFA), the service also applies appropriate validations, styling and layout to adaptive form fields during conversion.

**Signing Content.** With over 20 years of experience developing and refining PDF and signature technologies, Adobe is uniquely positioned to help organizations build legal and compliant signature processes in compliance with FedRAMP. With Adobe Sign, you can increase your Content Velocity by building routing workflows that include typical e-signatures, digital signatures, or both. Here are steps your organization can take:

- Combine e-signatures and digital signatures in a single document or form while controlling who signs where, and in what order.
- Automate workforce-driven digital signature processes that use Personal Identity Verification (PIV) cards or Common Access Cards (CAC) — or mobile credentials.
- Complete and sign self-serve forms anywhere, on any device without installing additional software.

While the majority of Adobe Sign use cases are integrated into existing software-as-a-service (SaaS) applications, more sophisticated use cases might require advanced forms and workflows (Adobe Sign and AEM Forms working together).



# ZERO TRUST CONTENT SECURITY

Protecting Adobe and customer data and systems is at the core of Adobe's Content Strategy. As the security landscape grows increasingly complex and challenging, traditional perimeter-style security architectures need to be rethought, especially within national security — this has given rise to new architectures, like Zero Trust, that take a different approach.

By assuming that nothing is trusted inside or outside the perimeter, Zero Trust aims to dynamically verify all access to system resources. With Adobe Experience Manager (AEM) Content Security (Digital Rights Management - DRM), Zero Trust principles can be extended down to the content level and provide much stronger protections and mitigations against potential issues. Overall, content security helps:

- Prevent compromised computers and networks from leaking sensitive content such as PII, CUI, FOUO, etc.
- Prevent authorized users from redistributing sensitive and high value digital content through digital and print copies
- Prevent unauthorized users from opening documents, no matter how they received them
- Remove the need to rely on shared-password protections on each document
- Change or revoke the authorized users of any document, without republishing it
- Leverage any existing users, groups, roles or attributes for limiting authorization
- Restrict printing, modifying and copying
- Revoke all copies of a document
- Use analytics of protected documents for business intelligence and counterintelligence



# CYBERSECURITY LANDSCAPE

In many organizations, including government, security has largely focused on perimeter-style defenses, such as multiple network zones, firewalls and encryption. As we adjust to new realities such as working from home, traditional security begins to fall short in today's digital environments. Your organization may need 256-bit content security that works across on-premise and cloud (Amazon Web Services, Microsoft Azure, Office 365, Teams, SharePoint, etc.) environments and is vendor agnostic.

Faced with protecting sensitive content and documents, organizations turn to encryption methods, as evidenced by security compliance frameworks that encrypt data at rest and in motion. Yet, all encryption methods aren't equal. Agencies must evaluate each approach against the threat models for a given environment. For

instance, whole-disk encryption only defends against physical theft of the drive. Moving up the stack to network protection measures like Secure Sockets Layer (SSL), Transport Layer Security (TLS), or virtual private network (VPN) poses issues. Data is encrypted at one end, only to be decrypted at the other end and exposed to unauthorized activities. Application security measures like transparent encryption in the database are still prone to Structured Query Language (SQL) injection attacks and application exploits to access information.

To combat potential security threats, IT security practitioners have started adopting zero trust with content-level data protection technologies such as Digital Rights Management, which controls access by dynamically authorizing user permissions.

Adobe's Content Security integrates with Attribute-based Access Control (ABAC) solutions to enforce granular access to portions of sensitive documents dynamically, based on user and informational asset security attributes.



# HOW DOES CONTENT SECURITY WORK?

Proven both commercially and in public sector (used across more than 30 government organizations), AEM Content Security can persistently protect content and data independent of storage and transport at scale with Federal Information Processing Standard-140 Suite B encryption. Once content security is applied, the content security policy can restrict user permissions dynamically (before and after, content has left the network) like read, print, copy, modify and sign throughout the data lifecycle, even when data is removed from the portal or records management system. Policyholders set an offline lease period for content and also enable a one-time "Mission Impossible" policy for instant destruction after content is read.

When a user attempts to open a file, a request (only the Document ID is sent, not the entire document) is made to DRM Server to determine whether or not the user has access or not and what permissions the user has. Once these decisions are made the application sends a decryption key to the document viewer to open that document. The decryption of the document occurs in memory when the user opens the document but is automatically re-encrypted when closed for persistent protection. If you would like, a dynamic watermark can be added with a date and timestamp — so your content updates automatically each time it's updated or opened.

**Automated Encryption & Policies.** Encryption and policies can also be applied in an automated fashion to ensure data protection as part of an organization's process for Microsoft Teams or SharePoint. Content Creators can quickly and easily apply the appropriate security attributes to informational assets in a repository such as

AEM Assets. Paragraphs, images, videos, titles, and even bullet points can be assigned multiple security attributes like classification level, International Traffic in Arms Regulations (ITAR), and environmental variables. Once tagged, assets can be referenced in assembling content for consumption in Sites or Documentation XML.

**Sites and Documentation XML.** A report authored in Documentation XML as a web page may include text, images, and video, each containing different security markings. AEM Content Security integrates with the enterprise classification markup tool—Dynamic HTML (DHTML) version—to apply marking to an individual piece of content. When users authenticate into the system to view the report, they encounter dynamic redaction and see only the portions that they're authorized to see, based on their own security attributes, and authorization and libraries in the community. If any asset changes within the repository, such as reclassification of a video, all pages referencing that asset are automatically updated accordingly. If needed, the system can also enable end users to click.

**Out-of-the-Box.** AEM Content Security supports numerous authentication protocols (CAC, PIV, PKI, SAML, LDAP, Active Directory, login.gov, and one-time password OTP authentication), Federal Information Processing Standard-140 Suite B encryption, and a variety of file/formats out of the box such as Microsoft Word, Excel, PowerPoint, and PDF. If other file types are needed for protection, custom extensions, plug-ins, or applications can be developed using the Document Security software development kit (SDK).

# USE CASES

“Zero Trust” is a security concept centered on the belief that organizations should not automatically trust anything inside or outside its perimeters and instead must verify anything and everything trying to connect to its systems before granting access. There are three great use cases for moving toward a Zero Trust environment with content-level data protection:

1. The Department of Homeland Security's (DHS) Continuous Diagnostics and Mitigation ([CDM](#)) program for tools needed to protect sensitive information and high-value assets (HVA).
2. Building upon the first use case, the second focuses on helping organizations to quickly, easily, and securely share sensitive information with remote teleworkers on

- government, contractor, and even personally owned computers, phones, and tablets.
3. The third case is how the Department of Defense (DoD) strengthened its supply chain by protecting defense content. Recently, the DoD developed the Cybersecurity Maturity Model Certification ([CMMC](#)). CMMC builds upon Defense Federal Acquisition Regulations Supplement (DFARS) [Clause 252.204-7012](#), Safeguarding Covered Defense Information and Cyber Incident Reporting.

These three use cases are underpinned by complying with the National Institute of Standards and Technology's Special Publication 800-171 ([NIST SP 800-171](#)).

# CONTENT INTELLIGENCE

In the beginning, we talked about how the Content Velocity use case helps organizations inject efficiencies into every step of the content lifecycle, from asset creation, to organization, to automated delivery, and, crucially, all the way through to data-driven experience optimization. That last step is where Adobe Analytics comes in, augmenting the experience creation, management, and delivery functionality of AEM Sites, AEM Assets, and Forms with enterprise-grade content performance and analytics to maximize the performance and ROI of our customer's content efforts.

AEM Assets has out-of-the-box reporting, but Adobe Analytics provides capabilities like an

Analysis workspace to help understand customers, democratize insights, and streamline report and data sharing techniques. Adobe Analytics also provides advanced segmentation tools to create customer segments and build calculated metrics to show rolling averages. With Adobe Analytics, users can also access Flow Visualization dashboards to visualize customer movement, uncover next steps from entry, exit, or any other point in the journey, and easily create segments of users who follow a selected path. By supplementing the dynamic content delivery engine that is AEM Sites, Assets, and Forms with comprehensive data-driven performance optimization, organizations can ensure they are not only getting content quickly, but getting the right content, to the right people, at the right time.

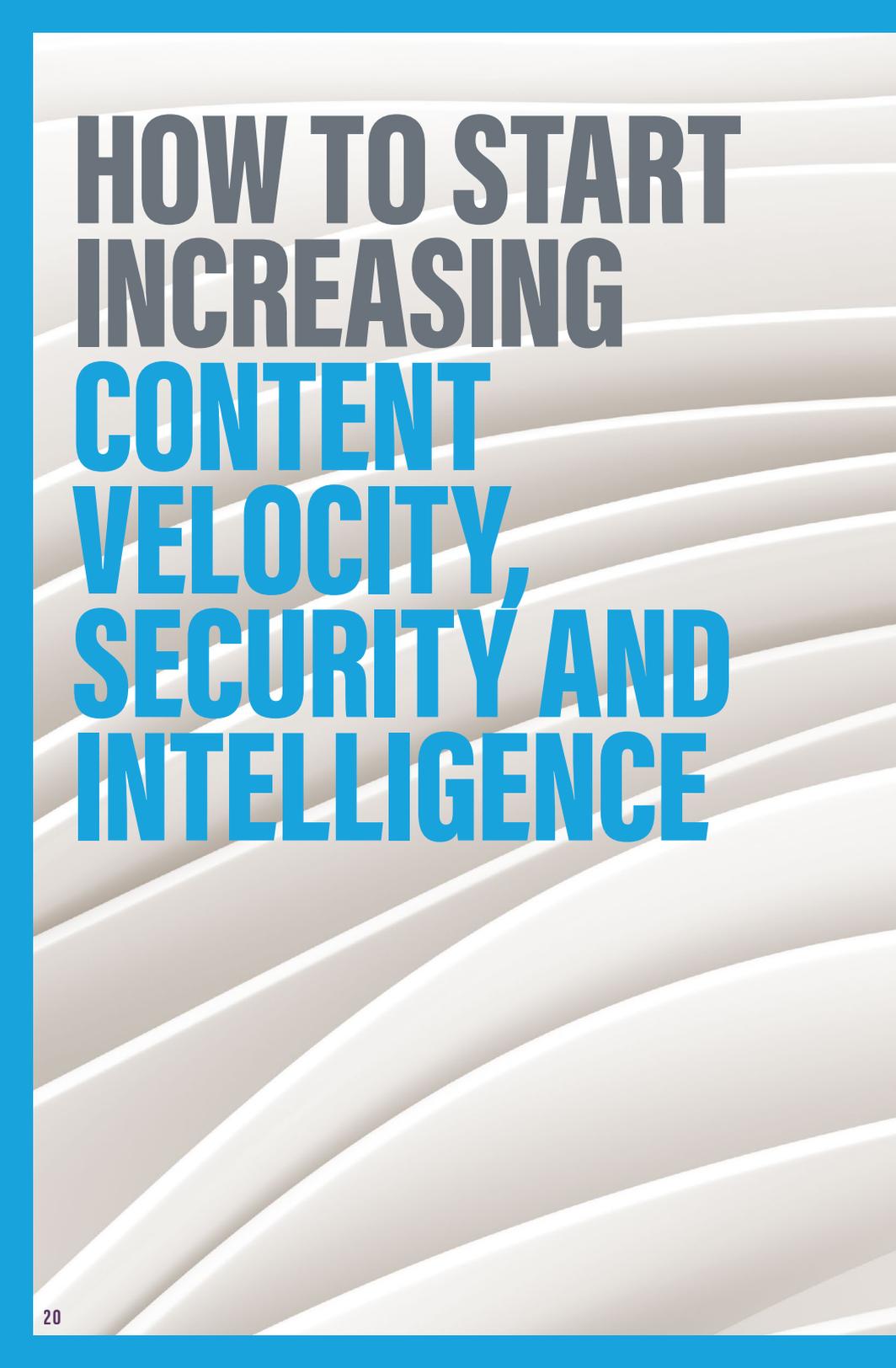
# CONTENT SECURITY AUDITING AND ANALYTICS

Content interactions in real-time provide much-needed data-driven insight for not only Business Intelligence, but Counterintelligence. For instance, what time and from where did Alice print that document? Did Bob read the last page? Or copy content from the document?

**Counterintelligence.** The centralized audit information includes both successful and unsuccessful document opens, as well as print, modify, form fill, and other attributes. This is coupled with unique document identifiers, filenames, usernames, date/time and IP addresses of interaction. This information is analyzed real-time to identify access and exfiltration attempts of sensitive information. It can be correlated with baseline history of previous consumption patterns and with other data sources. DRM and analytics help identify when unusually high number of document downloads, opens, or prints are taking place. It can also determine suspicious behavior based on time/day/location attributes. For example, giving access to a document by a user from their normal location during typical working hours would be granted, but access from a new location at different working hours might initiate an out-of-band authentication (phone call, mobile phone push request, etc.) before granting access. During incident response, it can quickly provide forensic information on potentially affected users, documents, and systems.

By going into AEM Content Security policy controls, you can revoke a document, disable a document, or even provide a new version update. If revoked or disabled, when users who have pre-distributed copies of the document open it, they are alerted that the document is disabled or revoked.

**Business Intelligence.** The same audit data can also provide document publishers with greater insights on how and where their content is being consumed across digital channels including websites, portals, blogs, email and other content sharing systems. This provides greater granularity and detail than just the number of downloads from the primary distribution source. All subsequent document accesses that are passed along and shared are able to be analyzed and correlated. This can highlight document popularity and affinity compared with other documents.



# HOW TO START INCREASING CONTENT VELOCITY, SECURITY, AND INTELLIGENCE

If your organization aims to improve content and delivery, it's essential to lay the foundation for more — more content, more accessibility, and delivered with more velocity than ever. To achieve those goals:

## 1. ASSEMBLE A CONSIDERABLE CONTENT LIBRARY

To keep pace with customers' content demands, you need a sizable, preexisting stockpile of content, including text, images, and video, that has been curated and meta-tagged.

## 2. GET A DIGITAL ASSET MANAGEMENT (DAM) SYSTEM IN PLACE

Resist the urge to keep using siloed Band-Aid solutions. When you look at all the different content needs an organization requires, it becomes obvious that Content Creators teams need to have access to a shared, central repository to allow them to reuse and repurpose things quicker.

## 3. GET ANALYTICS DATA

Having lots of data is important. But to deliver with relevance and speed means understanding what works and what doesn't (e.g., what content has been engaged with, what content generated a successful response, and what content customers want more of). This is the foundation for matching content with customers for the business experience wave.

## 4. APPLY AI AND MACHINE LEARNING

There are so many opportunities to introduce AI into your environment, especially when using a standards-based, open architecture such as AEM. AI can also be applied to the production of content. For example, you can use AI to intelligently crop and resize an image for an ad, enabling the real-time delivery of perfectly sized content. AI can help with the conversion of static, online forms.

## 5. AUTOMATE PROCESS AND WORKFLOWS

To keep up with customer content demands, it's essential to automate delivery workflows — this isn't something more people can keep up, especially as content demands grow. As organizations demand more with the same resources, they will need to deliver more content that's more relevant — and they'll have to do it at a faster pace than ever. To ensure your brand stays in-step with these demands, it's essential to keep iterating and keep refining your processes.

With Adobe solutions, agencies have seen year-over-year savings in resources and increases in Content Velocity. Adobe tools work together to help the national security community manage today's digital content with context at the speed of mission.



# Modernize mission-readiness with Adobe.

Create & collaborate securely  
with confidence.

By standardizing on Adobe solutions, the law enforcement and security community can maintain mission-readiness in a constantly changing environment by:

- Accelerating content creation to enable the mission
- Focusing on a user-centric digital experience
- Shifting toward a zero-trust architecture

Reimagine the digital experience with solutions for web modernization, online forms, digital asset management and content security. Learn what Adobe can do for your agency.

Learn more at:

[https://www.adobe.com/industries/government/  
law-enforcement-national-security.html](https://www.adobe.com/industries/government/law-enforcement-national-security.html)



# REIMAGINE YOUR DIGITAL EXPERIENCE

## *An interview with Michael Barr, Sales Director, National Security Group, Adobe*

The National Security Community is responsible for quickly identifying and reporting potential foreign threats before they happen – and that’s no small feat. Whether the threats are physical or cyber in nature, the many agencies involved in preventing and responding to them must be able to communicate and share resources to be most effective.

Data silos and information security concerns often get in the way of that ability, however. Information gets stuck in email inboxes, silos make business processes inefficient, poor data quality limits accessibility, and a lack of standard data formats means agencies can’t use data among applications, let alone among one another. Modernization efforts can go a long way toward eliminating those obstacles.

“The organizations within national security have always looked for ways to harness and adopt technology in support of its mission,” said Michael Barr, Sales Director, National Security Group, Adobe. “More recently, this community has increased focused on presenting an ever-relevant, dynamic and customized experience as opposed to static, moment-in-time views. While better gaining insights will be the foundation of this community’s adoption of technology, there is more prioritization to mission-oriented user experience.”

Several factors drive this change. Some of the more obvious ones are the ability to work from remote locations, as the pandemic has shown; rising workforce expectations; and policy mandates. But other, more subtle, factors also make change inevitable. They include the need for cross-organizational integration and collaboration; being mission-ready in a constantly changing environment; protecting the information to be shared, especially outside the community; and enabling a unified, agile and trusted workforce.

Still, knowing what’s needed and implementing it aren’t the same.

“Much like the various factors driving change within this community, there are various reasons complicating the use of solutions,” Barr said. “Many agencies are challenged by a mix of technologies that serve limited purposes. That leads to complications, as what works for one agency may not work for another. To manage a vast amount of data, people and process, these organizations have thousands of operational systems and servers, which can make for a siloed workforce. Another factor may be the necessary (and sometimes mandated) individual security requirements within each organization.”

***“Reimagining your digital experience for your mission or business operational systems is more than automating existing functionality. It is a critical exercise in ensuring that the needs of the business, user, and existing technical systems are reached, especially when migrating to the cloud.”***

***—Michael Barr, Adobe***



A solution such as Adobe Experience Manager (AEM) that is based on open and industry standards can address those challenges. It is platform-independent, allowing for integration with other platforms, providing users an enterprise-ready central hub to enable the management, curation and collaboration of images, videos, documents, manuals and audio clips in a web-based repository. It is designed to accept all types of content, categorize that content using rich metadata structures and present that content in a user-friendly interface based on those metadata structures.

That kind of flexibility is crucial because it “allows for progress to be made incrementally and not an ‘all or nothing’ outcome seen from purpose-built open source customizations,” Barr said. “Reimagining your digital experience for your mission or business operational systems is more than automating existing functionality. It is a critical exercise in ensuring that the needs of the business, user, and existing technical systems are reached, especially when migrating to the cloud.”

Given the sensitive nature of the content that the national security community deals with, security is of the utmost importance in any DAM solution they use. A data-centric security solution such as AEM goes beyond the encryption that form the foundation of most agencies’ security structures. It also applies attribute-based access control to allow granular access to portions of sensitive documents, document auditing and analytics, and digital signatures, which automate integrity and authenticity checks on sensitive content.

“At the heart of the digital experience is security that can be integrated into some of the complex policies and mandates,” Barr said.

Today, national security and law enforcement agencies need to create a cohesive information ecosystem that enables them to collect, manage and share digital assets efficiently and securely.

# CASE STUDY: AEM ASSETS IN ACTION



## *How the communications team at Sandia National Laboratories uses AEM Assets to streamline work.*

With a primary mission of protecting the U.S. nuclear arsenal, Sandia National Laboratories is not immune to the collaboration struggles most government agencies face.

Steve Pope, a Graphic Designer, and Business Systems Analyst who works in Sandia's communications group, said that he and his team often struggled to find and share assets.

"We'd get these reply-all emails [in which] our designers, communication teams would be looking for an asset or an image, primarily the original or a native file," Pope said. Once, 32 people were on one e-mail, with someone asking where to find an asset and respondents saying that they didn't know.

The team would look for file names, but scattered naming conventions used throughout the lab's siloed shared folders made it nearly impossible. For instance, a document with graphs showing spending information could be saved as "graphs," "charts," "spending," or any number of things, depending on the whim of the worker.

Similarly, internal and external customers, such as the Energy Department and other national labs, would ask for a specific graphic to update. "Most of the time they've got a 72 dpi image that they put on the web or on a [Microsoft] PowerPoint slide and we've got to go find it because that person may or may not have been in our group or did work with our group at one time or was a contractor helping us out," Pope said. "If we don't have the original, then we have to spend the time recreating and making it look right as opposed to spending a little time just updating."

Something had to change to decrease the time the team spends retrieving assets from shared drives, various collaboration solutions and myriad storage locations. So, about four years ago, they implemented the Adobe Experience Manager platform, including AEM Assets, which lets users manage and share their digital assets, such as images, videos, documents and audio clips, in a web-based repository. It also provides robust metadata for searching, curating, categorization and project management. Sandia also uses the AEM Assets Desktop App, which makes the assets in AEM available on the local desktop for use in native desktop applications.



"It's basically helped us build a bridge [and] close the gaps of communication with our communications team by providing resources, tools, capabilities for our entire group and our customers within Sandia," Pope said of AEM.

"We're also able to provide pockets of teams the capabilities to manage their own assets and keep those locked down to just their communications teams and their customers so they can file-share, share assets easily, research and find those things. It's brought an enterprise tool to our communications because, like I said, those reply-all emails, they're not communications. They're more of an annoyance."

Pope and the Sandia team were able to configure and customize AEM Assets to fit into the team's system and government policies, procedures, security and applications. "We were able to sit down, look at the code, look at the documentation, figure out how do we apply X and Y to make Z," Pope said.

Once installed, AEM Assets allowed the team to determine how to develop a taxonomy and set a plan for managing files, permissions and controls so that users could have control over their specific areas, while there's also enforcing enterprise-level controls. Security has improved as a result, Pope said, "because without a login, employees can't access the system."

Additionally, AEM helps digitize tribal knowledge around particular assets and project as personnel comes and goes. AEM allows users to see the comments, workflows, versions, source files and changes that have resulted in its current state.

"A lot of the colleagues I met when I began are leaving or have retired, and I've noticed...that Joe used to know XYZ and he taught this new guy X and Z but he left out Y. How do we capture that?" Pope said.



AEM Assets helps because users can tag and enter metadata such as who's in a photograph, when and where it was taken, and even how it could best be used. It's important to have not only a taxonomy, but also project IDs, titles, descriptions and tags on content so that it becomes easily available over time because the more that we add to our content, the more it will become usable for our organization, said Tyson Bowman, Senior Solutions Consultant at Adobe.

"Our file sharing and our collaboration, where we can store all of our quick guides, our how-to's, even templates, some of the old photographs..., the archiving, all that has been able to be bridged by using Adobe Experience Manager Assets," Pope said. "It's really helped us fill the gap because not just through attrition, but if somebody like Karen wakes up one day, hits the lottery, [and] decides she's going to turn off her cellphone, never speak to anyone again, we have a way to go in and find her files."

But getting to this point has taken effort. Pope said training and employee buy-in were crucial because it was a matter of cultural change as much as technological. For example, he created a team to

think about what they would search to find a given photo and then tag as much metadata as they can.

Pope said he also has to prompt people across the lab to use Adobe Digital Asset Management. Because there are so many workers with their own specialties and ways of working, introducing a new step requires what Pope calls a "constant reminding process." "When someone says, 'I wish we could do this,' and I say, 'We have AEM already. You should be using it,'" he said. "Once they realize it's there, they do it."

That's because it's easy to use. It's online and feels like a website, he said. "You just type what you want and boom! There's your results."

Today, Pope's team is better able to focus on the task at hand because they experience far fewer interruptions from clients seeking help with finding assets. What's more, they don't have to waste time on duplicative work.

"Change is the No. 1 concept in life. You have to adapt," Pope said.



# CHEAT SHEET

Current challenges to a seamless, integrated digital experience in the National Security Community:

- Legacy technology that perpetuates data silos
- Poor data quality and standardization
- Nonstandard file formats that can't be shared
- A mix of technologies each of which serves specific, but often limited purposes
- A limited workforce to manage a seemingly unlimited amount of data, systems and processes
- Security considerations, given the sensitive nature of national security content

## 5 BEST PRACTICES FOR IMPLEMENTING A DIGITAL ACCESS MANAGEMENT SOLUTION AND WHY YOU SHOULD

Today, content is no longer static, so using file systems meant for static files won't drive the collaboration, workflow and security that a national security agency needs to disseminate timely insights or experiences. A DAM solution is the dynamic approach organizations need. Here are tips for implementing them:

- Define your digital foundation.
- Implement with content velocity in mind.
- Use a governance model that supports change.
- Define your implementation-specific life cycle.
- Define your content types.

# CONCLUSION

**National security agencies have long had modernization on their radars. Although they've made investments in new technologies, the sheer volume of data, the need for mobility, and an expanding threat surface have complicated the situation. DAM, coupled with zero-trust content security, is a game-changer. It centralizes the management of those pain points and shifts the traditional security focus from one area (the perimeter) to the entire environment.**

**With the right DAM solution, the IC can break literal barriers to create a unified information ecosystem that lets them achieve the three goals of creating frictionless business processes, moving toward a zero-trust architecture, and fostering collaborative communications.**

***THANKS TO  
ADOBE FOR THE  
SUPPORT IN  
PRODUCING THE  
PUBLIC SECTOR  
RESOURCE.***

THEIR

HIS

OR



## About Adobe

Adobe's trusted and proven enterprise solutions enable next-generation digital government. Government agencies can leverage Adobe's industry leading enterprise end-to-end data management and customer experience platform that supports modern websites, digital forms and electronic signatures. From the first stages of creative design to the full customer journey, Adobe can help agencies fully modernize so they can better reach the public and their employees and provide greater access to programs and resources.

To learn more visit us at: [adobe.com/government](https://adobe.com/government)

To view our resources in response to the COVID-19 pandemic go to: [adobe.com/covid-19-response/government-resources.html](https://adobe.com/covid-19-response/government-resources.html)

Adobe and the Adobe logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.



## About GovLoop

GovLoop's mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

For more information about this report, please reach out to [info@govloop.com](mailto:info@govloop.com)



1152 15th St. NW Suite 800  
Washington, DC 20005

P (202) 407-7421  
F (202) 407-7501  
[www.govloop.com](http://www.govloop.com)  
[@GovLoop](https://twitter.com/GovLoop)

