Kiteworks

Federal and National Governments: 2023 Sensitive Content Communications Privacy and Compliance

Industry Findings and Takeaways

HIGHLIGHTS

Communication Tools in Use	13%	7+
	27.5%	6
	45.5%	5
	14.5%	Less than 4
Average Annual Budget for Communication Tools	9.4%	$500,000+
	13%	$350,000 – $499,999
	40%	$250,000 – $349,999
	35%	$150,000 – $249,999
	2.5%	$100,000 – $149,999
Number of Third Parties With Which They Exchange Sensitive Content	7.5%	5,000+
	26.5%	2,500 – 4,999
	58%	1,000 – 2,499
	4.5%	499 – 999
	3.5%	Less than 499
Attack Vector Weighted Score (based on ranking)	100	Password/Credential Attacks
	72	Cross-site Scripting
	69	Denial of Service
	63	Session Hijacking
	59	Rootkits
	58	URL Manipulation
	57	DNS Tunneling
	49	Malware (ransomware, trojans, etc.)
	49	Zero-day Exploits and Attacks
	48	Man in the Middle
	37	Phishing
	30	SQL Injection
	25	Insider Threats
Exploits of Sensitive Content Communications in Past Year	7%	10+
	16%	7 – 9
	54%	4 – 6
	22%	2 – 3
Level of Satisfaction With 3rd-party Communication Risk Management	14%	Requires a New Approach
	24%	Significant Improvement Needed
	38%	Some Improvement Needed
	24%	Minor Improvement Needed

Growing Cyber Threat Landscape in Federal and National Governments

Federal and national governments are prime targets for cyberattacks. Federal and national governments collect and exchange highly sensitive information, run applications used by millions of citizens and businesses, and manage critical infrastructure. Disruption of federal and national government applications and operations can have an enormous impact—from theft of state secrets to interruptions in critical services. Targeted sensitive information includes large volumes of personally identifiable information (PII), business information, defense sector information, intellectual property (IP) related to state-sponsored infrastructure and resources, and more. Even though the U.S. federal government ranks number one in the world in its commitment to cybersecurity,[1] significant gaps exist. For example, the U.S. Government Accountability Office (GAO) has issued 236 recommendations since 2010 for 24 different U.S. federal agencies to strengthen specific data privacy practices. However, a recent report found that 60% remain unaddressed.[2] And it is not simply the U.S. federal government with cause for concern.

Too Many Disaggregated Sensitive Content Communication Tools

Like private-sector enterprises, federal and national governments rely on a disproportionate number of communication tools for sending and sharing sensitive content. Kiteworks' 2023 Sensitive Content Communications Privacy and Compliance Report found that over 85% of federal and national governments admit they rely on five or more tools. The need to acquire and manage disparate communication tools requires more budget allocation and resources to manage. But more importantly, a communication tool soup prevents federal and national agencies from establishing uniform policies for tracking and controlling sensitive content communications. In addition to ratcheting up risk, this also makes it immensely more difficult to adhere with cybersecurity mandates and data privacy regulations.

85.5% of federal government agencies use five or more tools for sensitive content communications.

Assessing Third-party Content Communication Risks

Federal and national government agencies face considerable challenges when it comes to third-party content communication risks. 92% of them exchange sensitive content with over 1,000 third parties. When asked to list their communication channels that pose the greatest risk, federal and national government respondents to the Kiteworks survey report listed web forms as the channel with the highest risk (54.5% of the respondents gave it a rank of 1, 2, or 3), which was followed by file sharing (49.5% of the respondents gave it a rank of 1, 2, or 3) and email (44.5% of the respondents gave it a rank 1, 2, or 3).

77% of federal and national government agencies experienced four or more breaches of sensitive content communications within the past year.

Risk mitigation is a serious problem for federal and national governments. Only 17% indicated they have implemented a comprehensive system to monitor and control access to sensitive content folders across all departments and content types. Alarmingly, 77% said they experienced four or more breaches of sensitive content communications within the past year. Unsurprisingly, over three-quarters recognize they must enhance their approach in managing third-party content communication risks: 62% indicate the need for significant or some improvement, whereas another 14% call for a new approach.

Assessing Content Communication Risks On-premise and in the Cloud

Much attention has been paid by federal and national governments on cloud security in recent years. For sensitive content communications, the risk appears to remain per our survey respondents. Almost 7 out of 10 admitted they do not have the capabilities to monitor and control content collaboration and sharing in the cloud. They are not doing much better on-premise with slightly less than half (46%) indicating they have such in place for on-premise file and email data communications.

Digital Rights Management for Sensitive Content Governance

Federal and national government respondents have a significant distance to go when it comes to the governance of sensitive file and folder access. Only 15% said their organizations monitor and manage third-party access across all departments, tracking activities such as who viewed a document and when, who accessed it and when, who downloaded it and when, and who shared it and when. Slightly more (17%) admit they manage and restrict third-party access to sensitive folders and files using capabilities like content permissions, expiration, locking, and versioning. These findings demonstrate that much work remains to be done around digital rights management (DRM).

The inability to view and edit any kind of content is listed by respondents as the top stumbling block (31% ranked it #1 and 32 ranked it #2) when it comes to DRM adoption, higher than any other industry sector. More than half of federal and national government respondents indicated alignment of their risk management strategy with sensitive content communication privacy and compliance is a priority for them over the next year.

Kiteworks for Federal and National Government Agencies

The Kiteworks Private Content Network is an ideal solution for federal and national governments seeking to unify sensitive content communications and institute zero-trust policy management for DRM and implement advanced security capabilities. First, it is also easy to use for internal government users as well as third-party contractors. FedRAMP Authorized and SOC 2 certified six consecutive years, IRAP Assessed to PROTECTED Level in Australia, ISO 27001, 27017, and 27018 certified, and Cyber Essentials Plus certified, among others, Kiteworks supports the world's leading cybersecurity standards. Second, unlike most other communication tools that use multitenant cloud hosting, Kiteworks is hosted on a single tenant and is unaffected by multitenant cyberattacks and breaches. Third, Kiteworks uses end-to-end encryption for each communication channel, ensuring that sensitive government data remains secure during transmission and at rest. Fourth, Kiteworks offers granular access controls, allowing governments to precisely manage who can access specific data. Fifth, Kiteworks provides detailed audit trails and real-time monitoring capabilities, enabling governments to demonstrate compliance with these regulations and maintain transparency in their operations. Finally, Kiteworks provides a secure platform for sharing large data sets, which is often a requirement in government operations. Whether it's sharing and sending state secrets, collaborating and sharing research data and public records, or collaborating on critical folders and files, Kiteworks ensures that data is protected through comprehensive governance and security capabilities.

[1] Ani Petrosyan, "Leading Countries Based on Global Cyber Security Ranking (GCI) 2020," accessed July 7, 2023.

[2] "Cybersecurity High-Risk Series: Challenges in Protecting Privacy and Sensitive Data," GAO-23-106443 Report, February 2023.

Get the Full Report

Kiteworks

Kiteworks 2023 Sensitive Content Communications Privacy and Compliance Report

Seeking to empower private and public sector organizations to manage their file and email data communication risks better, Kiteworks began publishing an annual Sensitive Content Communications Privacy and Compliance Report in 2022. Rogue nation-states and cybercriminals recognize the value of sensitive content and target the communication channels used to send, share, receive, and store it—email, file sharing, managed file transfer, web forms, APIs, and more.

The 2023 Sensitive Content Communications Privacy and Compliance Report surveyed 781 IT, security, risk, and compliance professionals across numerous industries and 15 different countries. The in-depth report, which is based on their survey responses, explores a range of issues related to file and email data communication risks—how organizations are addressing those today and plan to do so in the coming year. The analysis includes a look back to 2022 data and what changes were observed in 2023.