Kiteworks

2024 Analysis of Sensitive Content Communications in the Federal Government: Security and Compliance Trends

HIGHLIGHTS

Communication Tools in Place	28%	7+
	3%	6
	28%	5
	7%	4
	24%	3
	10%	2
	0%	1
Exchange Sensitive Content With Third Parties	28%	Over 5,000
	10%	2,500 to 4,999
	24%	1,000 to 2,499
	7%	500 to 999
	31%	Less Than 499
Data Types Biggest Concern (Top 3)	61%	Legal Communications
	50%	IP
	44%	GenAI LLMs
	33%	PII
	33%	PHI
	33%	Financial Documents
	28%	M&A
	17%	CUI and FCI
Biggest Privacy and Compliance Focus (Top 2)	55%	Country-specific Data Privacy Laws
	45%	GDPR
	28%	U.S. State Privacy Laws
	24%	SEC Requirements
	21%	CMMC
	14%	HIPAA
	14%	PCI DSS
Most Important Security Validations (Top 2)	48%	ISO 27001, 27017, 27018
	45%	NIST 800-171/CMMC 2.0
	34%	FedRAMP Moderate
	31%	SOC 2 Type II
	24%	IRAP (Australia)
	17%	NIS 2 Directive
Number of Times Experienced Sensitive Content Communications Hack	17%	10+
	10%	7 to 9
	17%	4 to 6
	34%	2 to 3
	17%	1
	3%	Don't Know

The 2024 Kiteworks Sensitive Content Communications Privacy and Compliance Report provides an in-depth analysis of the challenges and trends in managing sensitive content across various industry sectors, including the federal government. This brief focuses on the key findings related to the federal sector, highlighting the tools used for sensitive content communications, cybersecurity concerns, third-party communication risks, specific cyber threats, and compliance implications.

Managing All the Sensitive Content Communications Tools

59% of federal government agencies rely on five or more communication tools to send and share sensitive content, which is more than the full cohort average (53%). When it comes to tracking and controlling sensitive content, 59% of federal respondents said they can track and control sensitive data sent and shared internally; the same percentage indicated they can do so when it is exchanged externally. Both are slightly better than the full respondent averages of 51% and 43%, respectively. This may be due to the different security controls and standards instituted at federal government levels.

When it comes to sensitive content communications privacy and compliance priorities, preventing leakage of confidential IP and corporate secrets was by far the highest priority for federal respondents (69% listed it as either their top priority or second-highest priority). Outside of legal firms, this was the highest industry response rate for this priority. The percentage is much higher than the full cohort percentage (56%). Avoiding regulatory violations and associated fines and penalties and mitigation was the second most-frequently cited priority—likely related to the different standards with which federal agencies must now comply (e.g., CMMC 2.0, Executive Order 14028, etc.).

Assessing the Third-party Risk of Sensitive Content

Managing third-party risk is an important priority for federal agencies, with 38% reporting they exchange sensitive content with over 2,500 third parties (lower than the global cohort at 44%) and 60% doing so with more than 1,000 third parties (slightly less than the full respondent average of 66%). When it comes to tracking and controlling sensitive content once it leaves an application, the federal sector is one of the more mature industry sectors with 62% indicating they can track and control over three-quarters of sensitive content when it leaves an application.

Assessing the State of Sensitive Content Compliance

86% of federal respondents revealed their measurement and management of compliance for sensitive content communications requires some to significant improvement. This was slightly less than what all respondents reported: 88%.

The government sector in general is very focused on data privacy of individual citizens and residents. In the case of our survey, country-specific data privacy laws were ranked first or second by federal respondents 55% of the time—dramatically higher than the full respondent 21% average. GDPR was next on the list at 45%.

When it comes to vetting and selecting security validations or certifications, federal respondents cited ISO 27001, 27017, and 27018 as their top priority (48%) followed by NIST 800-171/CMMC 2.0 (45%). Government security standards apply not only to the private sector but also the public sector, and thus a continued rise in these numbers is expected.

Assessing the Risk of Sensitive Content Security

80% of federal agencies indicate their measurement and management of security risk associated with sensitive content communications requires significant or some improvement; 20% said they require no improvement. The latter is higher than most other industry segments. But as the data breach data reveals, simply having a higher confidence level does not equate to lower risk.

44% of federal respondents admitted their sensitive content was breached four or more times (27% said seven times or more). These are less than the cross-industry cohort where 32% admitted to seven or more data breaches and 55% said they had four or more. Perhaps this is an indication that federal government agencies are doing a better job managing risk than their private sector counterparts. Federal agencies are certainly in the crosshairs of bad actors, so this could be potential good news (a data point to watch in next year's survey).

Advanced security capabilities and practices such as encryption, multi-factor authentication, and governance tracking and control are only used for some sensitive content by federal agencies slightly more than half (52%) of the time (measurably better than the global cohort that was at 41%)—39% admitted to some and 2% said none. Once again, this reveals a higher security maturity on the federal sector compared to all respondents.

Assessing the Cost of Security and Compliance

One may associate data breach litigation costs with the private sector, but they also apply to the public sector. 35% of federal respondents said they spend over $3 million annually litigating data breaches. When it comes to litigation costs, the survey found 45% of federal respondents indicated they spend over $3 million annually. 7% of federal respondents admitted they do not know their annual data breach litigation costs.

Knowledge and Categorization of Data Types

45% of federal respondents indicated they tag and classify over three-quarters of unstructured data; this is slightly less than the full number of respondents where 48% admitted the same. When asked how much of their unstructured data needs to be tagged or classified, a discrepancy is revealed with 41% indicating 80% or more.

Imperative for Robust Sensitive Content Management in the Federal Sector

The Kiteworks 2024 Sensitive Content Communications Report highlights the critical need for robust management of risk and compliance in sensitive content communications in the federal government sector.

Federal respondents listed legal communications as their number one data-type concern (61%). This was followed by intellectual property (50%). With the ongoing onslaught of attacks targeting nation-state secrets, this response makes sense. These federal priorities contrast with the answers from the full cohort where financial documents were listed 55% of the time and legal communications 44% of the time.

Operationally, federal agencies spend a lot of time managing logs generated by the numerous communication tools they use to share and send sensitive content. 48% of respondents must reconcile over 11 (the same as the average of all respondents). 10% of federal respondents did not know how many logs must be reconciled. This compiles into a huge report logjam for federal agencies, though at a lower rate than private sector counterparts; 21% spend 2,000 hours or more annually while 56% spend over 1,500 hours.

Get the Full Report