WILMERHALE

Big Data in the National Security and Intelligence Sector

Big Data was born in US military and intelligence agencies. But the recent emergence of ever more powerful data collection, processing and analytics capabilities has revolutionized the role of Big Data in the fields of national security and intelligence. This sector is increasingly data driven, yet also increasingly overwhelmed by data. Both the government and its service providers must learn to capitalize on Big Data while avoiding its pitfalls. For companies and institutions in the national security and intelligence realm, Big Data is more than a new trend; it is a core competency.

PRACTICE AT A GLANCE

- WilmerHale's national security, government contracts, cybersecurity, privacy, transactional and communications lawyers counsel clients on the unique challenges that affect private-sector stakeholders that analyze and handle national security and intelligence information.
- We have substantial experience with the specialized laws, regulations and practices that define the relationship between government agencies and the businesses that service the national security and intelligence communities.
- Our team has decades of experience in key positions in national security and intelligence agencies, including former general counsels of the Defense Department, Central Intelligence Agency, and FBI and for the Director of National Intelligence; former Deputy Attorneys General; former Director and Chief of Staff of the FBI; and former US intelligence officers.

INDUSTRY-SPECIFIC ISSUES

Cybersecurity is central to national security: Advanced analytics transform vast unstructured collections of data into valuable natural resources and tools for projection of global power. With Big Data's emergence as the currency of global relations, cybersecurity—offensive and defensive—is essential to national security.

Corporate transactions involving defense and intelligence Big Data require specialized expertise: Companies handling national security-related Big Data are subject to unique contract requirements, regulatory burdens and risk exposures that must be addressed in pre-transaction diligence review and in merger, asset purchase and stock purchase agreements.

$1.6 Billion

Approximate fiscal year 2016 US Department of Defense expenditure on Big Data solutions and services.

Really Big Data: The US Defense Information Systems Agency (DISA) manages 3,000,000 users of more than 2,800 applications utilizing more than 3.7 petabytes of data storage.

Source: *DISA*

INDUSTRY-SPECIFIC ISSUES *continued*

Contractors support and conduct government data collection, processing and analytics: Government agencies with Big Data requirements rely on a network of private-sector contractors and subcontractors to provide the sensors and devices that gather data; the facilities, equipment and software to store and process that data into usable information; and the people, algorithms and analytical tools to produce intelligence that supports national security decisions.

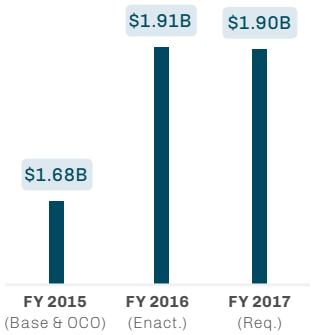
National security and intelligence information is pervasively regulated: Big Data in this sector involves sensitive information protected by a regulatory infrastructure that includes privacy laws, restrictions on sharing information among government agencies, industrial security safeguards for classified information, accreditation regimes for information systems and cloud services that handle government data, and restrictions on exports of controlled technical information.

EXPERIENCE

- Regularly advise information technology suppliers and service providers on defense and intelligence agency contract competitions, including evaluation of agency requirements, proposal preparation and bid protests.
- Advise defense and intelligence agency contractors and subcontractors on patent, software and technical rights in devices and software products used to collect, manage and analyze government data.
- Counsel for cloud services companies on the FedRAMP cloud service accreditation program, data location constraints, secure transmission requirements and continuous monitoring programs.
- Advise leading cloud service vendors on FAR and DFARS cybersecurity standards, cyber incident reporting requirements and "insider threat" program requirements.
- Advise information technology and analytics contractors on nontraditional contracting instruments available through the Defense Department's DIUx technology acceleration office; cooperative research and development agreements with federal laboratories; "other transaction" agreements with DARPA, IARPA, HS-ARPA and ARPA-E; and In-Q-Tel technology investment agreements.
- Negotiated data-use agreements and joint venture partnership agreements to provide companies with access to agency-maintained unstructured data.
- Advised a producer of unmanned aerial vehicle software on the terms of Defense Department and subcontract license agreements.
- Represented a major technology consulting services company in an agency's investigation of employees' handling of government data.
- Advise numerous producers of cryptographic devices and software on global export control compliance and licensing requirements.

"Big data has proven to be more than a buzzword — it continues to be a big priority for agencies within the Department of Defense, creating opportunities for contractors who can add to intelligence gathering, analysis and cybersecurity."

— C4ISRNET



TOTAL DoD BIG DATA SPENDING AND BUDGET REQUEST, FY 2015-2017

— Source: FY 2015 DoD Budget Request

For more information visit us at wilmerhale.com/big-data | contact us at big.data@wilmerhale.com

18_0374 4/17