Hogan Lovells

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

Government contracts: Year in review and issues to watch in 2019

February 13, 2019

Agenda

- Cybersecurity for government contractors
  - Statutory developments
  - Controlled Unclassified Information (CUI) program
  - Department of Defense (DoD) cybersecurity rules
  - Federal supply chain
  - FAR cybersecurity rules
  - Trends for 2019
- Data rights for government contractors
- Aerospace, Defense, and Government Services (ADG) mega-mergers
  - 2018 M&A trends and 2019 outlook
- Questions


Cybersecurity for
government
contractors

Key cybersecurity developments in 2018

TOPIC
Statutory developments
Controlled Unclassified Information (CUI) program
Department of Defense (DoD) cybersecurity rules
Cybersecurity in the federal supply chain
FAR privacy training rule/PII breach rule
Trends for 2019

Statutory developments

FY 2018 NDAA

FY 2019 NDAA

CISA 2018

Statutory developments

2018 NDAA (Pub. L. 115-91)

- **Sec. 1634. Prohibition on use of products and services developed or provided by Kaspersky Lab**
  - Implemented by FAR clause 52.204-23, 83 Fed. Reg. 28,141 (July 16, 2018)
- **Sec. 1656. Security of nuclear command, control, and communications system from commercial dependencies**
  - First action by Congress to ban Huawei, ZTE, and affiliates' products/services in federal supply chain
  - Prohibits DoD from procuring any such items one year after enactment of the NDAA

Statutory developments *(continued)*

2019 NDAA (Pub. L. 115-232)

- **Section 881. Permanent Supply Chain Risk Management Authority (codified at 10 U.S.C. §2339a)**
  - Makes permanent the authority provided by Section 806 of the 2011 NDAA
  - DoD can exclude contractors based on supply chain concerns; such exclusions are not reviewable in a bid protest before the GAO or in federal court
- **Sec. 889. Prohibition on certain telecommunications and video surveillance services or equipment**
  - Ban on federal agencies procuring Huawei, ZTE, or affiliates' products/services beginning one year after enactment of NDAA

Statutory developments *(continued)*

FY 2019 NDAA (Pub. L. 115-232)

- **Sec. 1639. Procedures and reporting requirement on cybersecurity breaches and loss of personally identifiable information [PII] and controlled unclassified information [CUI]**
  - DoD to establish procedures to promptly give Congress notice in the event of a significant loss of (i) personally identifiable information (PII) of civilian or uniformed members of the armed forces, or (ii) controlled unclassified information (CUI) by a cleared defense contractor
- **Sec. 1655. Mitigation of risks to national security posed by providers of information technology products and services who have obligations to foreign governments**
  - Requires IT contractors disclose to DoD situations where a foreign person and/or government has been allowed to review the code of such products, services, or systems within five years prior to the enactment of the 2019 NDAA or anytime thereafter

Statutory developments *(continued)*

- **Cybersecurity and Infrastructure Security Agency Act (CISA) of 2018** (Pub. L. 115-278)
  - Amended the Homeland Security Act by adding Title XXII, *Cybersecurity and Infrastructure Security Agency*
  - CISA redesignated the National Protection and Programs Directory (NPPD) of DHS as the Cybersecurity and Infrastructure Security Agency (CISA)
  - CISA will operate the National Cybersecurity and Communications Integration Center (NCCIC), provide cybersecurity incident response assets, and mitigate cybersecurity risks and threats to critical infrastructure

Controlled Unclassified Information (CUI) program

Federal Controlled Unclassified Information (CUI)

CUI final rule

- National Archives and Records Administration (NARA) CUI Final Rule (September 14, 2016) now codified at 32 CFR Part 2002 *Controlled Unclassified Information*
  - The final rule states that agencies "***must*** use NIST SP 800-171 when establishing security requirements to protect CUI's confidentiality on ***non-federal information systems*** [*i.e., contractor internal information systems*]."
  - Final CUI rule clarifies that "information a non-executive branch entity possesses and maintains in its own systems ***that did not come from, or was not created or possessed by or for***, an executive branch agency or an entity acting for an agency" is not CUI.
- DoD is still the only agency specifically addressing CUI safeguarding via standard contract clauses (DFARS 252.204-7012)
- However, the regulations on safeguarding CUI do apply to all federal agencies

CUI program 2018 developments

- FAR case No. 2017-016 *Controlled Unclassified Information* (opened on 4/13/2017) will extend the federal CUI program requirements in 32 CFR Part 2002 to contractors
  - Until the FAR contract clause on CUI is adopted, contractors may find themselves subject to potentially conflicting and duplicative agency-specific agreement provisions regarding CUI
- NARA has been revising the categories published on the CUI Registry
  - Nine (9) New DHS categories officially added to CUI Registry (given "Provisional Approval" by NARA on Sep. 7, 2018)

DoD cybersecurity rules

DFARS clause 252.204-7012

New DoD guidance

DFARS safeguarding rule

Overview

- DFARS clause 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting* (Oct 2016):
  - Applies to ***all*** DoD contractors and subcontractors, including small business and commercial item contractors…
    - …***except*** contracts for the acquisition "solely" of COTS items.
  - Requires covered contractors to:
    - 1) adequately safeguard "Covered Defense Information" (CDI) and
    - 2) "rapidly report" cyber incidents.
- Requirements flow-down; the DFARS clause must be included in subcontracts potentially involving CDI

DFARS safeguarding rule *(continued)*

Security

- Contractors are required to provide "adequate security" on all covered contractor information systems (i.e., systems with "CDI")
  - "CDI" means DoD unclassified controlled technical information (UCTI) or other information types on the federal CUI Registry that is –
    - (1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or
    - (2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.
  - "Adequate security" means, at a minimum, implement ***all*** of the security requirements in NIST SP 800-171 *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* by no later than December 31, 2017
- Can submit requests to DoD to provide alternate solutions to 800-171 requirements
  - i.e., a control is not applicable or contractor proposes an alternative measure

DFARS safeguarding rule *(continued)*

Incident reporting

- Covered DoD contractors must "rapidly report" any "cyber incident" that "affects a covered contractor information system [or] the [CDI] residing therein…"
  - Rapidly reporting is defined as within **72 hours** of the contractor's discovery of the cyber incident using the reporting fields at https://dibnet.DoD.mil
- ***Subcontractors*** must also:
  - Rapidly report cyber incidents directly to DoD
  - Notify their prime contractor (by providing them with the DIBNet incident report number)

2018 developments

New DoD guidance

- Defense Pricing and Contracting, DoD Guidance for Assessing Compliance and Enhancing Protections Required by DFARS Clause 252.204-7012 (November 6, 2018)
  - Guidance to acquisition personnel on assessing contractor's approach to providing adequate security → potentially reviewing system security plans (SSPs) and plans of action and milestones (POAMs) when such plans are required by the solicitation or contract to be provided to DoD (e.g., CDRL)
- New OUSD (A&S) guidance
  - Sample SOW language addressing access to/delivery of contractor's SSP and flow downs to suppliers
- Assistant Secretary of the Navy (ASN) Memorandum Implementation of Enhanced Security Controls on Select Defense Industrial Base Partner Networks (September 28, 2018)

Federal supply chain

Ban on Kaspersky Labs

Bans on Huawei and ZTE

Federal supply chain

NDAA requirements

- **Ban on Kaspersky Lab, Inc. (Kaspersky Lab) products and services**
  - FAR clause 52.204-23 *Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities*
- **Ban on Huawei and ZTE**
  - DFARS case 2018-D022, *Covered Telecommunications Equipment or Services*, will implement 2018 NDAA Sec. 1656
  - FAR case 2018-017, *Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment*, will implement 2019 NDAA Sec. 889
- **Disclosure of foreign review of source code/products**
  - DFARS case 2018-D064, *Disclosure of Information Regarding Foreign Obligations*
- **Section 881**
  - Makes permanent the authority of DoD to exclude high-risk sources under the previously enacted "Section 806" authority
  - DFARS case 2018-D072 *Extension of Supply Chain Risk Management Authority*

FAR cybersecurity rules

Privacy Training rule

(Upcoming) PII breach rule

FAR final rule on Privacy Training

- Issued on December 20, 2016, but effective January 19, 2017. 81 Fed. Reg. 93,476
- Under the contract clause, **FAR 52.224-3, *Privacy Training***, contractors are responsible for ensuring that training is completed by their employees that:
  - Have access to a "system of records" under the Privacy Act of 1974;
  - Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle PII on behalf of an agency; or
  - Design, develop, maintain, or operate a system of records.

FAR final rule on Privacy Training *(continued)*

- This rule is broader than just the Privacy Act, for which there have been FAR clauses for many years…
  - e.g., FAR clause 52.224-1, *Privacy Act Notification;* 52.224-2, *Privacy Act*
- This rulemaking states the "required training ***does not encompass solely the Privacy Act***; ….it is only ***one of the areas*** listed that must be addressed as part of privacy training."
- Bottom line – organizations that had federal Privacy Act training for employees have generally had to update their training (and agencies are still updating their own training)

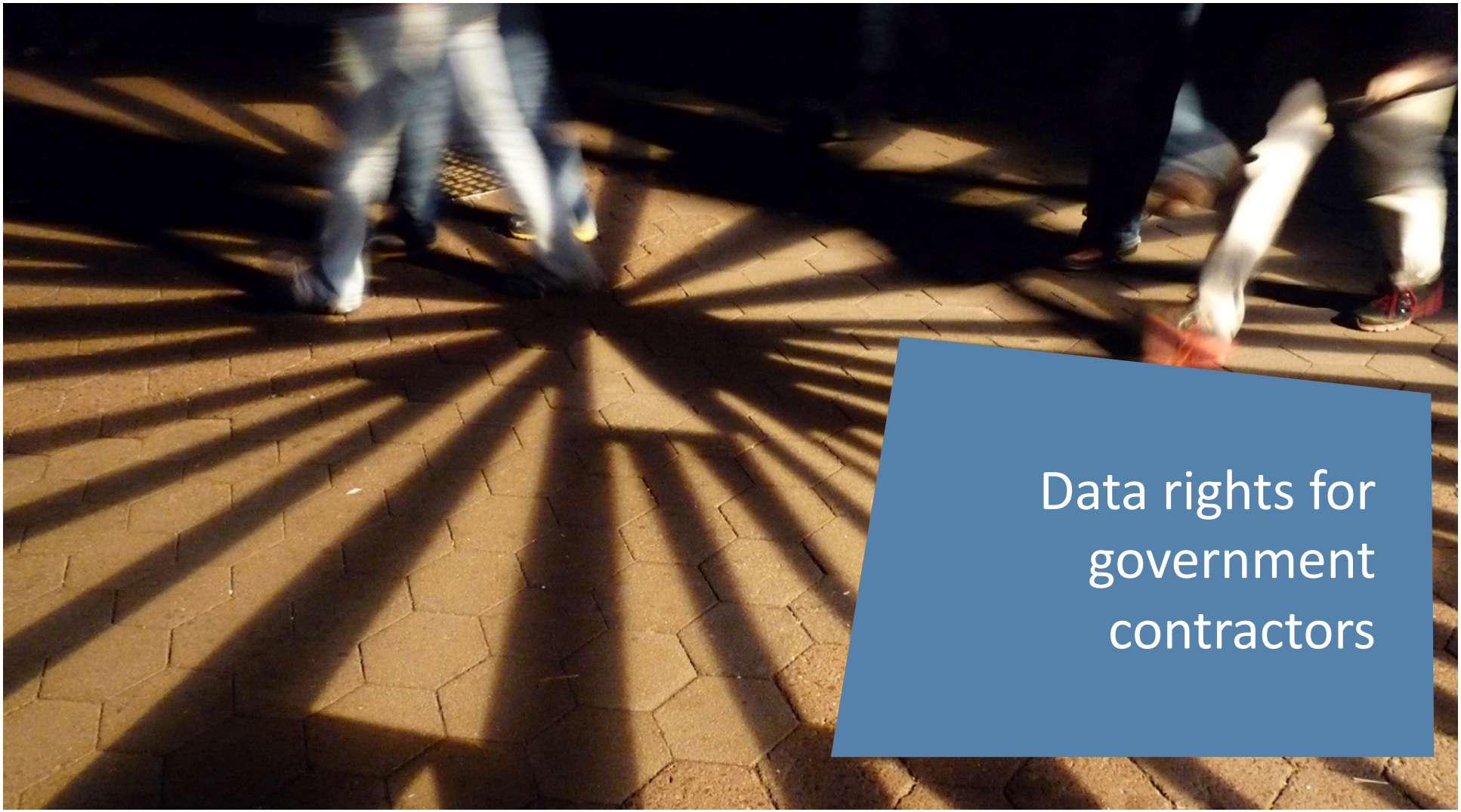
FAR privacy training linked to FAR breaches of PII rule

- One of the training topics that must be covered under FAR 52.224-3 are procedures to be followed in the event of a suspected or confirmed breach of PII
- The FAR clause directs contractors to OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*
- M-17-12 directs agencies to require their contractors and subcontractors (at any tier) to:
  - properly encrypt PII;
  - report a suspected or confirmed breach in accordance with agency procedures; and
  - allow for inspection, investigation, forensic analysis, and any other actions necessary to comply with OMB M-17-12 and assisting the agency with responding to a breach.
- FAR case No. 2017-013, *Breaches of Personally Identifiable Information* will extend OMB M-17-12 requirements to contractors
  - As of this writing the FAR case still has not be published in the Federal Register for public comment

Trends for 2019

Looking ahead – Cybersecurity trends for 2019

- Increased DoD scrutiny of contractor cybersecurity posture
  - DCMA audits; DoD IG also announcing audits
  - Cyber as a source selection criteria → DPAP guidance document strongly recommending DoD customers to use cyber as a criteria
  - Providing your SSPs and POAMs for DoD review
- Potential security controls above and beyond DFARS clause and 800-171
  - Navy memo: enhanced security controls; NCIS to install sensors on contractor's network when intelligence indicates a vulnerability or potential vulnerability
- Increased pressure on primes to manage their supply chains
  - DCMA to review whether primes flow down DoD CUI requirements to suppliers
- Final FAR clause on CUI (?)


Data rights for government contractors

Data rights – Definitions

- "Data" when we talk about "data rights" includes:
  - **1. Technical data**
    - Recorded information only
    - Does not apply to the item or component itself
    - Does not include financial, cost, pricing, management, or contract administration data
    - Includes data bases and computer software documentation
  - **2. Computer software**
    - "Computer programs that comprise a series of instructions, rules, routines, or statements, regardless of the media in which recorded, that allow or cause a computer to perform a specific operation or series of operations;" and
    - "Recorded information comprising source code listings, design details, algorithms, processes, flow charts, formulas, and related material that would enable the computer program to be produced, created, or compiled."
    - Excludes data bases and computer software documentation (which are "technical data")

Allocation of data rights

- Contractor retains title to the data, but grants the government a license to use the data.
  - Note that even the government's "unlimited rights" are not *exclusive* rights. The contractor retains the ability to use or license others to use unlimited rights data or software
- The government license can take one of the following forms, starting with the least restrictive to the government:
  - Unlimited rights;
  - Limited rights (for technical data) or restricted rights (for computer software); or
  - Government purpose rights (DoD).

Government Expense? ***Unlimited rights***	**Private Expense?** ***"Limited rights" / "restricted rights"***
Mixed USG / Private Expense? ***Government Purpose Rights (DoD / DFARS)*** ***Unlimited Rights (FAR)***	

Allocation of data rights *(continued)*

- **Unlimited rights**
  - Government gets rights to use, disclose, reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly in any manner and for any purpose to have or permit others to do so
  - Government gets unlimited rights in data first produced in performance of the contract or data delivered under the contract
  - Unlimited rights does not prevent contractor from using the data
- **Limited rights**
  - Government gets rights to reproduce and use within the government data that the contractor developed at private expense (trade secrets or confidential)
  - Contractor may have the option to withhold delivery of limited rights data
  - Government may negotiate specific use rights with the contractor

Allocation of data rights *(continued)*

- **Restricted rights – applicable to computer software**
  - Government may
    - use or copy for use with the computer for which it was acquired
    - use or copy for use with a back-up computer
    - reproduce for safekeeping
    - modify, adapt, or combine with other software
    - disclose to and reproduce for use by support service contractor for the above purposes

Allocation of data rights *(continued)*

- **Government purpose rights (GPR)**
- DoD only (DFARS 252.227-7013) – generally used when there is non-segregable, mixed funding
- The right to use, modify, disclose, or release technical data/software:
  - within the government without restriction and
  - outside the government for government purposes (including procurement) as long as third party recipient agrees to use and NDA that limits use to government purposes (e.g., Foreign Military Sales (FMS))
- Note that after a finite period (currently nominal five year period), GPR data converts to **unlimited rights data**

2018 developments

- VT Halter Marine, Inc., B-415510.2 (Jan. 2018)
  - Evaluation credit based on data rights
- Cubic Defense Applications, Inc., ASBCA No. 58519 (May 2018)
  - Includes lengthy historical discussion of data rights
  - Application of that discussion to a dispute concerning a settlement agreement

Data rights – Common issues

- Are the data markings appropriate?
  - Universe of data to be marked may be subject to negotiation
  - Must provide notice and mark data exactly as required or risk a grant of unlimited rights to the government ("Mark it or lose it")
    - **Unlabeled data (or *incorrectly labeled data)* can become unlimited rights data**
- When must the FAR/DFARS clauses be flowed down to subcontractors?
  - The **FAR** does not require flow-down of the FAR data rights clauses…but the contractor is required to obtain from subcontractors all data and rights necessary to fulfill government contract obligations
  - The **DFARS** expressly provides for the mandatory flow-down to subcontractors of a number of contract clauses pertaining to technical data and computer software, including, for example the basic rights in noncommercial data and computer software clauses, and clauses relating to the government's right to challenge restrictive markings

Some best practices

- **Develop appropriate business processes to ensure the use of appropriate restrictive markings**
  - The FAR and DFARS set forth the markings contractors must apply to their technical data and computer software in order to indicate the relevant funding sources and adequately protect that data and software. DFARS 252.227-7013(e); DFARS 252.227-7014(e).
  - Include in proposals an appropriate list of data and/or software delivered with less than unlimited rights
  - Timely respond to all government follow-up inquiries related to markings
  - Notably, with respect to DoD contracts, there is a presumption that commercial items were developed at private expense, which presumption will not be questioned unless facts indicate otherwise. DFARS 252.227-7037(b).

Some best practices *(continued)*

- **Assess your accounting system and how the system is used for development projects**
  - Focus is on ensuring that the system allows your company to adequately support claims of development at private expense
  - For example, are there job/project codes sufficient to identify internally funded development work? Are those codes used consistently by employees?
  - Job codes could also assist with marking internal work product such as test results, as being in support of a privately funded development effort
- **Develop appropriate business processes to ensure that data/software is not inadvertently delivered to the government**
  - For example, develop procedures to reduce the likelihood of technical team members inadvertently making deliveries outside of appropriate channels, e.g., through informal discussions with government technical personnel

IP and data rights – Some best practices

- **Maintain detailed records of development projects**
  - Maintain records relating to its development projects, particularly records regarding its funding sources for each. If questioned by a contracting agency or other entity, detailed records will help support a contention that an item, component, or process was developed at private expense.
  - Examples of such records might include the following:
    - Documents describing the parameters and goals of the development project at issue.
    - Project-related work plans and employee rosters.
    - Documents describing the identified funding source for each stage of the development project.
    - Documents supporting costs incurred for the development project (e.g., time cards, expense reports, vendor, and supplier invoices).
    - Project records and deliverables, such as reports and drawings, with dates and annotations indicating with which development project the record is associated.

Some best practices *(continued)*

- **Review contracts to identify which IP regime applies to your contract**
- Watch out for an agency or a prime contractor trying to include both FAR and DFARS clauses in the same contract
  - The DFARS and FAR data rights regimes developed independently through detailed statutory/regulatory history
  - The DFARS and FAR clauses cannot be reconciled if they appear together. The DFARS data rights clauses replace (and do not supplement) the applicable FAR clauses.
- Also be aware of non-DoD agency-specific clauses and other non-standard "one-off" clauses incorporated into contracts and other agreements
  - For example, the Department of Energy has agency-specific regulations governing the acquisition and use of technical data as well as copyrights in government contracts. *See* 48 C.F.R. Subpart 927.4 ("Technical Data and Copyrights")

Some best practices *(continued)*

- **Review contracts to flag the less common data rights clauses including:**
- FAR 52.227-16, Additional Data Requirements
  - Permits the government to order data first produced or specifically used in performance of the contract any time during contract performance or within three years after acceptance of all items to be delivered under the contract.
- FAR 52.227-17, Rights in Data – Special Works
  - This clause is broad, and gives the government unlimited data rights in all data delivered and first produced under the contract. It also limits the contractor's use of the data to contract performance, unless permitted otherwise by the government, and restricts the contractor's right to copyright assertion.
- DFARS 252.227-7027, Deferred Ordering of Technical Data or Computer Software
  - (Similar to FAR 52.227-16) Government can order any technical data or computer software generated during performance of the contract or under any related subcontract during contract performance and for three years after acceptance of all items to be delivered under the contract.


ADG mega-mergers

Harris Corporation/L3 Technologies, Inc.

Transaction details

- Harris and L3 to combine in all stock reverse triangular merger of equals
- Merger agreement signed 10/12/2018; expected to close in mid-calendar year 2019
- Equity value of transaction: US$15,770,000; Enterprise value: US$18,372,000
- L3 stockholders to receive a fixed exchange ratio of 1.30 shares of Harris common stock for each share of L3 common stock
- Price per share: US$201.33
- Upon completion of merger, Harris shareholders will own approximately 54 percent and L3 shareholders will own approximately 46 percent of new company
- Combined company will be called **L3 Harris Technologies, Inc.**

Harris Corporation/L3 Technologies, Inc. *(continued)*

Strategic benefits to deal

- Combined company will be sixth largest defense company in the United States; top 10 defense company globally
- Approximately 48,000 employees and customers in over 100 countries
- For 2018 calendar year, combined company was expected to generate net revenue of approximately US$16 billion, EBIT of US$2.4 billion, and free cash flow of US$1.9 billion

"The companies were on similar growth trajectories and this combination accelerates the journey to becoming a more agile, integrated and innovative non-traditional 6th Prime focused on investing in important, next-generation technologies…By unleashing this potential, we will strengthen our core franchises, expand into new and adjacent markets and enhance our global presence."

United Technologies Corporation/Rockwell Collins, Inc.

Transaction details

- United Technologies acquired Rockwell through a reverse triangular merger; announced on 9/4/17; merger completed on 11/26/2018
- Equity value of transaction: US$22,747,000; Enterprise value: US$29,954,000
- Consideration: US$140 price per share made up of US$93.33 in cash and $46.67 in United Technologies stock, subject to a 7.5 percent collar
- Upon completion of merger, United Technologies shareholders became owners of 93 percent of the combined company and Rockwell Collins shareholders became owners of 7 percent.
- Rockwell and UTC Aerospace Systems integrated to create new business unit **Collins Aerospace Systems.**

United Technologies Corporation/Rockwell Collins, Inc. *(continued)*

Strategic benefits to deal

- The acquisition is expected to generate an estimated US$500 million+ of run-rate pre-tax cost synergies by year four
- Post-closing, Rockwell and United's UTC Aerospace Systems were integrated to create a new business unit called Collins Aerospace Systems

"This acquisition adds tremendous capabilities to our aerospace businesses and strengthens our complementary offerings of technologically advanced aerospace systems…in a rapidly evolving aerospace industry by making aircraft more intelligent and more connected…The integrated companies' expertise in developing electrical, mechanical and software solutions will allow us to deliver more innovative products and services and provide greater value to our customers and shareowners…"

General Dynamics Corporation/CSRA Inc.

Transaction details

- General Dynamics acquired CSRA through a two-step tender offer and reverse triangular merger; merger completed on 4/3/2018
- Equity value of transaction: US$6,762,000; Enterprise value: US$9,754,000
- Consideration: US$41.25 price per share in all cash; originally US$40.75 per share in cash (after competing bid by third-party)

General Dynamics Corporation/CSRA Inc. *(continued)*

Strategic benefits to deal

- Combined business expected to generate approximately US$9.9 billion in revenue and double-digit EBITDA margins in the Government Technology Services sector
- General Dynamics expects transaction to generate estimated annual pre-tax cost savings of approximately 2 percent of the combined company's revenue by 2020

"The acquisition of CSRA represents a significant strategic step in expanding the capabilities and customer base of GDIT…CSRA's management team has created an outstanding provider of innovative, next-generation IT solutions with industry-leading margins. We see substantial opportunities to provide cost-effective IT solutions and services to the Department of Defense, the intelligence community and federal civilian agencies."

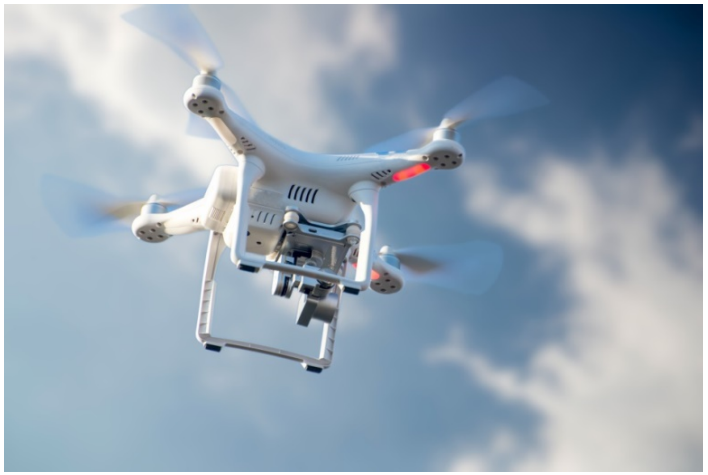
Veritas Capital/PWC's public sector business

- Veritas Capital acquired PWC's U.S. public sector business, a leading provider of strategic advisory services to customers such as the Department of Defense, Homeland Security, Veterans Affairs, Health and Human Services, the Department of State, and state and local governments.
- Carve-out transaction
  - Audited carve-out financial statements
  - Pre-transaction separation of business
  - Limited transition services
- Auction process and timing
- Post-closing

2018 M&A trends and 2019 outlook

ADG M&A in 2018

- 297* aerospace, defense, and government technology M&A transactions announced during 2018:
  - 82 transactions in the defense sector
  - 138 transactions in the aerospace sector
  - 77 in the government technology sector
- Consistent with levels seen in 2016 (294) and 2017 (299), but below the high in 2015 (315).



- Highly favorable budgetary environment continues to drive acquisitive defense and government services market.

*Figures from KippsDeSanto & Co. MarketView Winter 2019 Aerospace/Defense & Government Services Update

ADG M&A outlook for 2019

- Continuing trends:
  - Favorable budgetary environment
  - Acquirers search for targets whose capabilities align with federal spending priorities—cyber security, IT modernization, and cloud computing
  - Private equity buyers (e.g., Veritas, Arlington Capital) will continue to be active in the industry; accounted for 33 of 63 transactions in Q3 2018
  - Transactions among large primes force middle-market consolidation to remain competitive
  - Strong valuations
- Potential market disruptors:
  - Impact of mid-term elections
  - Government shut-down

ADG M&A outlook for 2019 *(continued)*

KippsDeSanto 2019 M&A survey

- Surveyed 222 dealmakers about M&A in the aerospace/defense and government services sectors
  - 122 CEOs, presidents, CFOs, corporate development executives, or other executive level respondents at corporate/strategic companies
  - 77 partners and senior professionals from PE groups
  - More than 60 percent of respondents are strategic buyers
  - 35 percent of respondents from PE groups

Expectations of M&A activity in 2019 compared to 2018

Defense

- 49.5 percent of respondents expect activity to remain about the same
- 23 percent expect activity to increase by 5-10 percent
- 4.6 percent expect activity to increase by more than 10 percent
- 4.6 percent expect activity to decrease by more than 10 percent
- 18.4 percent expect activity to decrease by 5-10 percent

Government services

- 47.8 percent of respondents expect activity to remain about the same
- 20.6 percent expect activity to increase by 5-10 percent
- 8.1 percent expect activity to increase by more than 10 percent
- 2.2 percent expect activity to decrease by more than 10 percent
- 21.3 percent expect activity to decrease by 5-10%

Aerospace

- 47.3 percent of respondents expect activity to remain about the same
- 22 percent expect activity to increase by 5-10 percent
- 7.7 percent expect activity to increase by more than 10 percent
- 5.5 percent expect activity to decrease by more than 10 percent
- 17.6 percent expect activity to decrease by 5-10 percent

M&A drivers

- When asked, "*What do you view as the most important factor influencing overall deal activity?*"
  - 78.4 percent responded: Defense spending/customer budget increases
  - 58.2 percent responded: Economic confidence
  - 55.8 percent responded: Public valuations/stock pricing
  - 53.2 percent responded: Credit markets/interest rates

Questions

Today’s presenters

Shamir Patel

Deputy General Counsel and Chief Ethics and Compliance Officer

spatel@guidehouse.com

Shamir Patel is the Deputy General Counsel and Chief Ethics and Compliance Officer at Guidehouse. Guidehouse is the former PwC government contracts business which was purchased in 2018 by Veritas Capital, a leading private equity investment fund, and now runs as an independent firm. Prior to moving to Guidehouse, Shamir was an attorney in the Office of the General Counsel at PwC for 6 years supporting the public sector, cybersecurity, and forensics practices.

Carine Stoick

Office Administrative Partner, Northern Virginia

T +1 703 610 6215

carine.stoick@hoganlovells.com

In today's increasingly interconnected world, global businesses require effective legal solutions that reach across borders and between continents. Carine Stoick, Office Administrative Partner of the Northern Virginia office and head of the Aerospace, Defense, and Government Services industry group's M&A subgroup, understands how to find and execute these solutions. She counsels companies and private equity investors on both domestic and cross-border corporate matters, including mergers and acquisitions, joint ventures, spin-offs, management and leveraged buy-outs, and corporate governance. From her experience advising clients both in the United States and abroad, Carine believes the best legal advice helps corporations and investors execute their business strategies no matter where their operations are located.

Practices

Commercial
Corporate
Corporate Governance
Joint Ventures
Mergers and Acquisitions
Private Equity

Today’s presenters

Michael Vernick

Partner, Washington, D.C.

T + 1 202 637 5878

michael.vernick@hoganlovells.com

Practices

Government Contracts
Education
Administrative and Public Law
Investigations
Litigation
Privacy and Cybersecurity
Public Procurement

Mike Vernick heads the firm's Government Contracts practice group and leads the Education industry sector team, which provides a full spectrum of legal services to colleges and universities. Mike has handled many of the most significant False Claims Act and qui tam cases involving federal research funds, several of which have involved potential exposure in excess of US$1 billion. His False Claims Act experience extends into all aspects of U.S. government contracts, including among others, cost allowability, GSA contracting, and commercial item determinations.

Michael Scheimer

Senior Associate, Washington, D.C.

T +1 202 637 6584

michael.scheimer@hoganlovells.com

Practices

Administrative and Public Law
Government Contracts
Intellectual Property
IT Law
Mergers and Acquisitions
Privacy and Cybersecurity
Public Procurement

Mike Scheimer advises clients on government contracts with a particular focus on national security, cybersecurity, and IT contracting. As a former defense contractor himself, Mike leverages his aerospace and defense industry network to maximize opportunities for clients. Mike has vast experience handling government contract cybersecurity issues, including comprehensive knowledge of cloud computing, data breach reporting, information sharing programs, and government information system security accreditation processes.

Hogan Lovells

www.hoganlovells.com