Business Insights in Trade Secret Management

Trade Secrets in Aerospace and Defense: a perspective

Shane O'Neill
Assistant General Counsel
Norsk Titanium

Company and Sector Specificities

1. Can you briefly describe your business and to what extent the protection of trade secrets is a crucial issue for you?

1.1. Business Overview and Size

Norsk Titanium AS (Norsk Titanium or company) was founded in 2007 to develop and commercialise significantly more affordable aerospace-grade titanium components. Specializing in additive manufacturing, specifically wire feed direct energy deposition, the company has grown into a global technology leader. The company began in Eggemoen, Norway, and expanded to the USA with large-scale manufacturing in Plattsburgh, New York. It employs about 120 people across both locations.

1.2. Active Sectors

Norsk Titanium is involved in the commercial aerospace, defense, and industrial sectors. Norsk Titanium's proprietary Rapid Plasma Deposition® (RPD®) process delivers high-quality material at an industrial production rate, targeting the titanium parts market for advanced applications like aerospace structures, defense, and engines. In the defense sector, the company has conducted extensive qualification efforts with General Atomics for unmanned aircraft systems, developing flight-critical structural components for next-generation platforms. The company is a qualified supplier for leading original equipment manufacturers (OEMs) and the only structural titanium manufacturer using additive manufacturing (also known as 3-D printing), approved by the U.S. Federal Aviation Authority (FAA) for commercial aircraft production. Additionally, the company supplies carrier trays that store and transport semiconductor wafers during their manufacturing process to ASML, the world's leading supplier of lithography machines for the semiconductor industry.

1.3. Importance of Trade Secrets

Trade secrets are an integral part of the company's intellectual property (IP) strategy, providing a cost-effective, flexible, and long-term competitive advantage. The company's trade secrets encompass technical, business, and negative trade secrets.

Technical Trade Secrets include those related to the company's proprietary RPD® technology, including: (i) material, process, and quality conditions and controls; (ii) manufacturing and process parameters and procedures; (iii) machine and equipment design, settings, and operation; (iv) qualification, inspection, and testing for manufactured parts; and (v) proprietary software source code and algorithms.

Business Trade Secrets include pricing models, cost and pricing information as well as business plans and strategies.

In addition, lessons learned and failures from nearly two decades of R&D, which, if disclosed, could enable competitors to develop similar technologies more rapidly are protected by negative trade secrets.

1.4 Sector-Specific Features Affecting Trade Secret Protection

The commercial aerospace market for the supply of wide- and narrow-bodied aircraft is a duopoly dominated by Boeing and Airbus. However, despite this, competition between these companies has intensified over the years with both companies vigorously competing for market share through continuous innovation and extensive investments. This competition allied with commercial pressure from airline customers (and broader environmental awareness around jet travel) seeking more fuel-efficient aircraft that offer an enhanced passenger experience has resulted in the development of new aircraft types.

The OEMS and their supply chain have responded to this challenge. Firstly, Boeing's launch of the 787 in 2009, makes extensive use of composite materials, represented a milestone in aviation technology, efficiency and passenger comfort, and latterly Airbus' A350 incorporates new technology increasing fuel efficiency by 25%. Further, more than two-thirds of this aircraft's structure is made of composite materials, light weight metals such as titanium, and advanced aluminium alloys.

Because of its light weight, high strength, durability and corrosion resistance, aerospace grade titanium alloy is used extensively in commercial aircraft manufacture. Traditional methods of manufacture (forgings and castings) of titanium alloy components have, depending on part geometry, a "high buy-to-fly ratio" (see below). Additive manufacturing, as explained below, reduces this.

In the aerospace industry, the amount of scrap material generated in production is referred to as the buy-to-fly ratio, which is defined as the ratio of the weight of raw material used to manufacture the part to the weight of the final part. The typical buy-to-fly ratio for aircraft structural parts is reported to be 20:1 (or higher), which means that for every kilogram of material that is flown on an aircraft, 19 kilograms are scrapped in the production process, resulting in many tonnes of scrap material from every aircraft that is manufactured. Another problem with machining from billet is the long lead time to procure the billets (billet is a term used in the manufacturing industry to describe a semi-finished product that is used to create various metal product) or forgings themselves, which can in some cases take more than a year.

Additive manufacturing (3-D printing), is the process of creating an object by building it one layer at a time. It is the opposite of subtractive manufacturing, in which a component is created by cutting away at a solid block of material until the final product is complete. Using additive manufacturing technology, it is possible to reduce machining costs and up to 50%-75% improvement in the buy-to-fly ratio compared with conventional methods: the cost savings are inherent in the technology.

Finally, the aerospace sector is one of the most regulated business sectors. The OEMs and their suppliers are subject to rigorous quality standards, particularly with respect to new technologies. Parts produced using additive manufacturing techniques are subject to a rigorous qualification and testing processes. . Further, the mandatory formal qualification process for defense and aerospace parts involves extensive empirical testing, which can be very costly and time-consuming. The qualification process involves considerable exchange of data with customers. This flow of technical data, which may include trade secrets, needs to be carefully monitored to ensure there is no "oversharing" and that the correct processes and procedures are in place to protect the company's proprietary interests in such data. Accordingly, new technologies, and their associated trade secrets, that reduce the cost, time, and complexity of producing qualified aerospace grade parts, while ensuring high quality standards, are crucial for the company (and additive manufacturers in the aerospace industry generally) and must be protected accordingly.

In addition, the company has to manage the complexities of working on projects that are subject to U.S. Government's federal and defence regulations as discussed below.

Internal Policies and Relationships

2. **What does your company consider when deciding to protect confidential information with trade secrets?**

Norsk Titanium takes a comprehensive approach to determining whether to protect confidential information as trade secrets or patents, which is detailed below.

2.1. Decision-Making Process

(i) IP Strategy Meetings, regularly held by the CEO, CTO, and members of the legal and IP teams.
(ii) Initial Trade Secret Status: Ideas and information are protected as trade secrets internally, from the moment of their inception.
(iii) Factors for Patenting vs. Trade Secrets:
- Patentability: Assessing if the invention is eligible for patent protection.
- Infringement Detection: Evaluating the difficulty of detecting patent infringement.
- Reverse Engineering: Considering how challenging it would be for competitors to reverse engineer the trade secret.

2.2. Trade Secret Management

Trade Secret Catalogue: Once designated as a trade secret, the invention is added to a catalogue that includes: (i) trade secret name and category; (ii) inventors' names and creation date; (iii) authorized employees responsible for the trade secret; (iv) access logging and expiry date; (v) details of where and with whom the trade secret is shared; (vi) electronic links to relevant documents; (vii) CTO consent for disclosure; (viii) details of changes to the trade secret.

2.3. Trade Secret Policy

Maintaining a comprehensive list of trade secrets is a foundational element of the company's trade secret policy. This policy outlines: (i) the role and importance of trade secret protection to the company; (ii) principles for access and storage; (iii) principles relating to disclosure to third parties; and (iv) treatment of third-party trade secrets.

2.4. Holistic Approach to Trade Secret Protection

The company has a holistic approach to trade secret protection involving intra-department collaboration, under which the Legal, HR, and IT departments each play a critical role.

- IT Department: (i) implements information classification system; (ii) applies industry-standard encryption measures; (iii) segregates trade secrets from non-trade secrets; (iv) implements access controls to prevent unauthorized access; and (v) restricts downloading, printing, and email distribution of trade secret information.

- HR Department
  (i) On-boarding: New employees are reminded of their obligations to maintain the secrecy of trade secrets, including those from previous employers; and
  (ii) Off-boarding: Departing employees, especially those joining competitors, must confirm that all inventions are properly assigned, return all electronic devices

containing trade secrets, and acknowledge in writing their obligation to keep trade secrets confidential.

- Employee Education and Monitoring
  (i) Training: Annual training provided by the Legal Department emphasises the importance of trade secret protection, the value it adds to the company, and that IP generated during their employment belongs to the company; and
  (ii) Monitoring: The company may consider whether to monitor patent applications and will put new employer on notice to the extent a departing employee has had access to confidential information.

- Non-Employee Access

Norsk Titanium does not provide trade secret access to non-employees, i.e., consultants or temporary employees, ensuring that sensitive information remains within the company.

External Policies and Relationships

3. **How do you manage specific risks to the confidentiality of your information arising from external relationships? How do you share your trade secrets?**

3.1 General management of confidentiality

The company takes a multifaceted approach to managing the confidentiality risks associated with external relationships, particularly concerning the sharing of trade secrets, as outlined below.

- Non-Disclosure Agreements (NDAs)
  (i) Standard NDAs: Confidential information is disclosed under an NDA. The starting point of documentation depends on the nature of the relationship. Standard NDAs typically include trade secrets within the definition of confidential information but may not provide specific terms for trade secret protection;
  (ii) Tailored NDAs: Specific attention is given to the terms of NDAs, especially when dealing with venture capitalists or investment banks; and
  (iii) NDA Limitations: The company emphasises having robust internal processes to compensate for any deficiencies in the NDA language.

- Internal Processes and Documentation
  (i) Document Labelling and Classification: All documents are labeled, clearly indicating proprietary or trade secret information to third parties; and
  (ii) Record Keeping: Detailed records are maintained when trade secrets are shared, including information about the counterparty, the agreement under which the trade secret is shared, and the termination date or certificate of destruction.

- Contractual Provisions
  (i) Incorporation of NDA Terms: In some cases, confidentiality provisions from NDAs are incorporated by reference into main agreements. In this instance it is imperative that appropriate consideration is given to the protection and treatment of trade secrets in the NDA. In others, standalone confidentiality provisions are included within the body of the agreement; and
  (ii) Sector-Specific Requirements: The U.S. defense sector, for instance, has stringent requirements for providing confidential material, which are adhered to rigorously.

- Approval and Marking
  (i) CTO Approval: Trade secret sharing requires approval from the CTO; and

(ii) Document Marking: Trade secret documentation and electronic files must be marked according to the document classification policy, which is supported by physical and cybersecurity measures.

3.2 U.S. Government Contracts

The company undertakes projects as a sub-contractor with prime contractors in the U.S. defense sector, subject to the Federal Acquisition Regulations (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS). These regulations govern IP handling, including trade secrets, in U.S. Government procurement contracts. For development projects, FAR and DFARS clauses define how the Department of Defense (DoD) can license contractor-developed IP, adding complexity to collaborations.

By way of background, in general, if a contractor develops a "*subject invention*," i.e., any invention of the contractor conceived of or first actually reduced to practice in the performance of work under the contract, the contractor can retain exclusive title to that subject invention if it discloses it to the government and complies with the patent application filing and notification procedures implemented under the Bayh-Dole Act by FAR Subpart 27.3. In exchange, the government receives "*a nonexclusive, nontransferable, irrevocable, paid-up license to practice, or have practiced for or on its behalf, the subject invention throughout the world*." FAR 52.227-11 also provides that the government can retain title under certain circumstances, such as if the contractor elects not to pursue a patent. If the U.S. Government obtains title to the subject invention, then the contractor retains a non-exclusive royalty-free license throughout the world for that subject invention.

The DoD's rights in technical data are a subset of IP issues whereby the DoD gains rights to the technical data, computer software, and computer software documentation developed under a DoD contract; *technical data* includes any *"data, other than computer software, that embody trade secrets or are commercial or financial and confidential and privileged, to the extent that such data pertain to items, components, or processes developed private expense, including minor modifications*". Therefore, it is easy to contemplate that any such technical data may comprise or include trade secrets.

Under DoD contracts, a subcontractor's rights to technical data provided to the government are governed by explicit contract provisions and the DFARS, which are referenced in the contracts. Subcontracts often incorporate by reference the contract clause "Rights in Technical Data-Noncommercial Items," as found in the DFARS at 252.227-7013. This clause grants the government certain rights to the subcontractor's IP. However, it may entail giving away more rights than desired by the subcontractor, potentially including trade secrets.

Contracts incorporating DFARS 252.227-7013 result in the U.S. Government obtaining three types of licence rights: (i) unlimited rights; (ii) government purpose rights; and (iii) limited rights.

Unlimited rights, which arise where development was funded exclusively at the government's expense, imply the 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, and to have or permit others to do so*".

When the government receives *government purpose rights (GPRs)* to a sub-contractor's technical data, the government may use the technical data in "*any activity in which the United States Government is a party*." In contrast to unlimited rights, a government purpose is **not** the right to "*use, modify, reproduce, release, perform, display, or disclose technical data for commercial purposes or authorize others to do so*". The government obtains GPRs in technical data developed under a procurement contract at the expense of both the contractor and the

government. GPRs usually expire in five years, after which the government retains unlimited rights.

In contrast to the above rights, in the event the U.S. Government receives limited rights to a subcontractor's technical data, it gains the ability to use, modify, reproduce, release, perform, display, or disclose the data **within its own operations**. However, it cannot disclose this technical data to external parties, including the subcontractor's competitors, without explicit written permission from the subcontractor. The U.S. Government typically obtains limited rights in technical data developed exclusively at private expense.

Unlimited rights, given for government-funded developments, pose a risk to the company's IP, as they cannot be kept as trade secrets. However, DFARS provide a mechanism for contractors and sub-contractors to protect their trade secrets. DFARS 252.227-7013, permits sub-contractors to protect their proprietary data by marking the data with protective markings such as restrictive legends or proprietary legends. That same DFARS clause requires the sub-contractor to identify and list certain data that are to be furnished with restrictions. Technical data either incorrectly marked or not marked at all cannot be protected from disclosure to competitors, with loss of any trade secret contained within.

3.3 Best Practices for Protecting Trade Secrets subject to FAR and DFARS

To mitigate against the risk of providing the U.S. Government with unlimited right, the company has adopted the best practices into its processes:

(i) Identifies what IP will be developed and the associated risks at the solicitation or proposal stage;
(ii) Prepares data rights assertions tables to explicitly state the rights the government will receive in technical data;
(iii) Thoroughly reviews contract terms with the prime contractor to understand IP expectations and ensure no additional clauses alter the government's rights or give additional rights to the prime contractor;
(iv) Properly marks technical data with the appropriate legend to prevent the government from claiming unlimited rights in projects not wholly funded by the U.S. Government;
(v) Executes NDAs with prime contractors or third parties seeking access to the company's technical data.

3.4 Jurisdictional Challenges

The company's strategy for protecting trade secrets across various jurisdictions is significantly influenced by U.S. law due to its U.S.-based customers and facilities, as well as the extensive jurisprudence on trade secret misappropriation in the U.S. The L'Oreal v. Olaplex case illustrates the importance of precise legal agreements, showing that NDAs are only a starting point. The judgment highlighted issues with ambiguous NDA language and insufficiently defined trade secrets, leading to unenforceability.

Accordingly, the company's processes and procedures are designed to align with considerations and practices that enhance the likelihood that its trade secret protection measures will be deemed appropriate by the courts.

4. **Following the end of the business relationship, to what extent do you implement specific measures to ensure the protection of your trade secrets (e. g., deletion of confidential information)?**

To secure trade secrets after the conclusion of a business relationship, Norsk Titanium implements strict measures: (i) limited sharing of trade secret information only with specific

individuals within the third party; and (ii) requiring the recipient to certify in writing that all trade secret material has been destroyed and no such information remains under their possession.

Enforcement Measures of Trade Secrets – Best practices for monitoring potential misappropriation and resolving disputes

5. **Do you implement any specific measures to monitor potential trade secret misappropriation?**

Norsk Titanium implements specific measures, including technical controls and continuous monitoring, to mitigate the risk of trade secret misappropriation. These measures are supported by employee training to foster a culture of awareness and accountability.

- Access Control Measures
  - (i) Role-Based Access Controls: Access to trade secrets is restricted based on the employee's role and necessity; and
  - (ii) Authorization and Logging: All access to trade secret information is logged and monitored to ensure compliance with access control policies.

- Network and Cybersecurity Monitoring
  - (i) Continuous Network Monitoring: The company has implemented continuous monitoring of its network to detect unusual activities that might indicate unauthorized access or data exfiltration.
  - (ii) Penetration Testing: Regular penetration testing of firewalls and other cybersecurity measures are conducted by external third parties to identify and address vulnerabilities in the IT systems.
  - (iii) Intrusion Detection Systems: These systems help in identifying and responding to suspicious activities that might signal an attempt to access or steal trade secrets.

- Employee Training and Awareness include: (i) regular employee training programs seeking to highlight the importance of protecting the company's IP; (ii) IP awareness campaigns directed to employees, underscoring the company's ownership of IP generated during their employment; and (iii) onboarding and offboarding processes, as detailed in paragraph 2.4. above.

- Patent Application Monitoring:
  The company does not monitor patent applications submitted by former employees, since it is deemed impractical and cost-prohibitive relative to the scale of the business.

6. **How do you resolve potential disputes regarding trade secret misappropriation?**

Norsk Titanium has not been involved in disputes regarding trade secret misappropriation.

The company does not have a formal policy on using arbitration or court proceedings for trade secret appropriation cases, opting instead for a flexible approach based on each case's specific circumstances. This approach is influenced by customer preferences, as some prefer arbitration while others prefer court jurisdiction.

Both court and arbitration proceedings have their merits and drawbacks, but for the company, the crucial factor is the ability to seek interim relief from courts in its business jurisdictions. This is especially important in trade secret misappropriation cases to immediately halt infringing actions and limit economic damage.

Interim relief must be available under applicable arbitral rules, though its effectiveness can vary, especially in urgent cases. During transaction negotiations involving trade secrets or technology, it's crucial to assess whether seeking interim relief from an arbitral tribunal or a national court is more advantageous. This assessment should consider the tribunal's power to grant interim relief and the practical enforcement of that relief in jurisdictions outside the arbitration seat.

The company has identified a number of practical points which may assist when responding to suspected trade secret misappropriation, including (i) maintaining readiness to initiate court proceedings or arbitration as necessary, including identifying suitable legal counsel with expertise in IP and trade secrets; and (ii) keeping records of all trade secrets, access logs, and any instances of potential misappropriation to support legal action if needed.