# National Security, Foreign Ownership and Defense Contractors

by Arun Sood

**When corporations have significant non-U.S. ownership, special arrangements are made to protect the classified information.**

U.S. national security interests require a determined and continuing attention to proper handling of classified information. This often requires restricting access to such information. On the other hand, technology and market considerations require that multiple corporations should have the ability to compete for classified work. When corporations have significant non-U.S. ownership, special arrangements are made to protect the classified information. This creates additional overhead in these companies, but this has not deterred these companies from undertaking classified work.

Multinational corporations often undertake classified contracts. This requires companies to adhere to rules that govern the exchange of data within the corporation, as well as restrictions on sharing of the information with corporate executives. These rules are typically incorporated into a special security agreement and approved by the Defense Security Service and the agencies for which the classified work is undertaken.

To understand the approach taken by such corporations and problems confronted by them, this article examines two companies: BAE Systems North America and Headstrong Public Sector Inc. The first is a very large multinational corporation: the second is a smaller company. Both companies undertake classified work. Their differences include diversity of customer base, fraction of revenue derived from classified work, type of work performed and type of ownership. The companies also have similarities: Both have some foreign ownership, operate in multiple countries and have become larger through mergers and acquisitions.

### BAE Systems North America

BAE Systems North America (BAE-NA), with headquarters in Rockville, Maryland, is a wholly owned subsidiary of BAE Systems. The parent company has its headquarters in the United Kingdom. The North American subsidiary has twenty-six thousand employees and annual revenue of $5 billion. BAE-NA is among the top ten defense contractors in the U.S. BAE worldwide has ninety thousand employees, with its largest employee base in the U.K. of fifty thousand and smaller operations in Germany, France, Saudi Arabia and Sweden. BAE-NA has targeted an annual growth rate of 25 percent. It manufactures and supplies high-tech equipment to U.S. government agencies. BAE-NA operates as a separate corporation with an independent board of directors. All the directors are U.S. citizens and have security clearances.

### Headstrong Public Sector Inc.

Headstrong Public Sector Inc. is a wholly owned subsidiary of Headstrong Corporation, with headquarters in Fairfax, Virginia. Headstrong Corporation is a $160 million company, with 2,600 personnel. In addition to several locations in the U.S., Headstrong has operations in India, Japan and the Philippines.

Headstrong Public Sector undertakes classified contracts. The Public Sector Division comprises forty-one personnel, twenty-eight of whom have clearances. Eight of the personnel hold high-level security clearances that allow work with intelligence agencies. Headstrong Public Sector's focus is on consulting services like enterprise architecture consulting, and even the classified work has a large high end consulting service component.

Although, BAE-NA and Headstrong are quite different, the classified work constrains the operations of both. The handling of the classified business was quite similar. This article identifies the common characteristics of the classified business operations of these companies. This focus potentially identifies characteristics that are generally applicable to firms doing classified work.

### Why Does the U.S. Government Contract with Such Firms?

The U.S. government wants the best technology at the lowest cost. The U.S. technology base is rich and competitive compared to other countries; however, in some niche technology areas other countries have an advantage. If a non-U.S. manufacturer develops hardware with similar functionality but a different manufacturing process and lower cost, then it benefits the U.S. when this knowledge is acquired. Costs can be contained by increasing competition in the marketplace—by encouraging military manufacturers headquartered in allied countries to build new facilities or acquire companies in the U.S.

In the commercial sector, the scale of production is often many times greater than military demand. For this reason, the military tries to use commercial off-the-shelf products. However, software and systems are complex. Many computer systems are manufactured and assembled in other countries. Monitoring the quality of these systems and ensuring that they do not have unauthorized software installed is a challenge. This encourages systems development in the U.S., where the processes can be better managed and supervised by personnel who have been vetted.

The United States wants to build consistent and reliable relations with allies, and to encourage the sale of U.S. military hardware, software, systems and technology to allies. This happens when companies headquartered in allied countries are given opportunities to invest in the U.S.

Companies serving the intelligence community have a particularly challenging task. If a U.S. company that serves the intelligence community merges with another company with significant foreign ownership, then often the acquiring company shifts its contracts to other firms that support the intelligence sector. On the other hand, the intelligence community interest in maintaining continuity of operations can often lead to arrangements in which related activity is compartmentalized and isolated. Government agencies have continuity of operations and reliable staff who understand the technology's applications.

### Why Is This Good Business for Commercial Firms?

Some foreign defense manufacturers focus on the defense market. These companies work with ministries of defense in their headquarters' countries. Investing in the U.S. helps manufacturers increase their revenue and diversify their client base. Such investments are usually encouraged by foreign defense ministries as a way of collaborating with U.S. defense manufacturers and strengthening relations with the U.S. government. Investments in the U.S. are also an easy way to get better access to the capital markets, especially the venture capital markets. Often an acquisition of a U.S. company provides the foreign investor rapid access to a technology base that has been validated and found appropriate in the defense environment. The company gets technical staff, which helps the company in technology transfer while continuing to meet security requirements of a federal agency. The company can apply this technology to other parts of its defense operations—potentially increasing revenue for the foreign-owned company.

In some cases, the defense or intelligence-related business merges with a larger firm. Why should a U.S. corporation with worldwide operations and significant foreign ownership retain a defense-related business? Consider the case of a corporation for which the defense and intelligence business is approximately 10 percent of its revenue base. Typically, the defense and intelligence agency clients are earlier adopters of technology, and hence performance on contracts for such clients can be used as an additional selling point with civilian and commercial customers. Technology developed for nonmilitary use can be readily moved to the secure world, but this requires increasing security levels. Additional security has increased appeal to the commercial and civilian government sectors. Successful implementation of systems in the more stringent defense environments is also recognized by foreign governments.

Some foreign-owned businesses pursue additional classified work because they want to employ a highly skilled and trained workforce. Consultants that serve commercial clients travel constantly, but those that serve a federal agency travel less—a factor in retaining high-value consultants.

### Organizational Constraints

Contracts for performing classified work flow to foreign-owned companies under a special security agreement between the company and the federal agency. Typically, all the work has to be performed in the U.S. In some cases, all the classified work is done at the client site, or at the site of a federal agency contractor who has the requisite site clearances. Foreign-owned businesses can request to have their facilities cleared for security if they can demonstrate that a clearance is necessary. Usually, the manager of the corporate division performing classified work has the necessary security clearances, and this person is the contact between the federal agency and the company. A division manager makes recruitment decisions for this division. Employees are U.S. nationals with appropriate clearances. The federal agency may also require that board members have clearances. Among the division corporate officers, the only person who could be a parent company representative is the chief financial officer. The security agreement also restricts the flow of information between the foreign owner and the division performing classified work.

The security requirements often stipulate a firewall between the classified and the unclassified operations of the company, and a firewall between the foreign owners and the group performing classified work. These firewalls also limit the information

that is available to the board of directors. The chief executive officer of the entity performing classified work has to have clearances. The security agreement may require that additional members of the board also have clearances. There are restrictions on the information that can be disclosed to the entire board. Most disclosures are restricted to generic explanation of the issues, and are generally related to financial and accounting performance issues. In some cases, the sponsoring agency may restrict that the agency name not be disclosed to the board members. The board can be told that an unidentified federal agency is disputing contract payments, but the board will not have access to the reasons that lead to the dispute. As part of the company's security agreement with the federal agency, the members of the board have to agree that they can perform their fiduciary responsibility without knowing the details of the classified work.

Classified work is not the only time that the board of directors makes financial commitments with only limited knowledge of the details. Privacy considerations also lead to similar constraints. Disputes with employees under the Health Insurance Portability and Accountability Act (HIPAA) have similar constraints. The HIPAA restricts the disclosure of the distribution of health-related information about the employees or their dependents to other parties. Thus, members of the board do not have access to such information and may have to make decisions without knowing the nature of the illness, the nature of the dispute or the reasons why the employee feels that the employer is responsible. The board has to decide based on terms of the settlement, litigation alternatives, related cost estimates and the extent of corporate liability. Typically, the corporate general counsel and the chief executive officer are the only members who have access to all details. The situation is similar for the entities undertaking classified work.

Other areas in which the board acts on the basis of limited information are in merger-and-acquisition and research-and-development investment decisions. Foreign-owned businesses in the classified work space often grow by merging with or acquiring a company in the appropriate work space. In this case, a division manager presents the relevance of the acquisition and the strategic growth plan. This includes technology assets acquisition, but not classified information. There are similar information disclosure constraints for R&D investments in the division performing classified work. Once again the board's role is strategic and includes approval of the financial implications.

The classified work space requires particularly stringent constraints on the acquisition of commercial off-the-shelf products produced in foreign countries.

### Intracompany Technology Transfer

Classified work gives the foreign-owned company exposure to higher-end technology. The deployment of this technology outside the classified work space may be an advantage to the company. However, because of the classified nature of the work, there are restrictions on the transfer of technology. Commercial off-the-shelf software acquisition illustrates the technology transfer possibilities. The classified work division acquires and integrates software, and it learns the functionality and limits of the software. Working with the vendor, work-arounds are developed. Unless there are specific national security concerns, this experiential information can be transferred to personnel not employed by the classified work division. On the other hand, application-related information cannot be exchanged with the other divisions. A copy of the software used in the classified arena may not be deployed outside the classified laboratory.

If the commercial software product has been integrated with other classified software, there are additional restrictions. In all cases the test is the impact of the transfer on national security, and the company must ensure that disclosure about the classified application or objectives is avoided; otherwise the government may debar the company from undertaking classified work. In this scenario, technical employees from the classified divisions are available to assist the adoption of commercial off-the-shelf technology for commercial and civilian government clients.

### Export and Import Rules

The export control regulations apply to all exports from the U.S. Vendors interested in exporting from the U.S. must comply with these regulations. In addition to export controls, the exporters of military hardware must also meet the International Trading in Armaments Requirements. These regulations are also applicable to technical meetings with personnel who do not have clearances.

Other regulations affect the import of software and systems. The intelligence community is careful of the software that is imported and installed on its computers. Software that may be acceptable in the context of the civilian government agencies may not pass the scrutiny of the intelligence community.

The classified work space requires particularly stringent constraints on the acquisition of commercial off-the-shelf products produced in foreign countries. A concern relates to development of software and hardware when there is no control of the development process. Since so much of electronic products and software development has been outsourced to foreign locations, it is difficult to assess the contents of the system. Other concerns include installation of worms, viruses, Trojan horses or sleeper software that is triggered years after installation on the computer. Often contractors are not allowed to use foreign-developed software in support of the intelligence community projects.

### Conclusions

By examining BAE Systems North America and Headstrong Public Sector key factors become apparent that are of importance to

the US government and the respective corporations in undertaking classified work. The early adopter reputation of these government agencies makes working for them particularly attractive to firms working in the high technology arena. However, classified work has to be undertaken in the context of a special security agreement, and this places restraints on operational, intra-corporate technology sharing and management disclosure. While all companies have to abide by the export control regulations, these companies must also abide by the stricter ITAR regulations.

The following are lessons for managing a defense contractor in the era of heightened national security:

- Companies undertaking classified work require an approved "special security agreement."
- Strict firewalls are required between classified and unclassified units of the company and between related companies.
- Members of the board have very limited access to information concerning classified projects.
- Military and intelligence agencies are early adopters of sensitive technology and are valuable customers for higher-end services.
- Compliance with laws governing security and export controls of sensitive data is mandatory. Through proper corporate policies and organization they can be met by both domestic and foreign firms.

**Arun K. Sood** is professor of computer science at George Mason University. He received his undergraduate degree at the Indian Institute of Technology, Delhi, and his master's and doctorate at Carnegie Mellon University. Photo of Sood (left) with former Virginia governor Mark D. Warner in India.