**ADDENDUM**
**NORWAY**

Our Code, as well as this addendum is provided as guidance in conducting your L-3 responsibilities. These documents are not intended to be all inclusive. You should seek guidance from the Legal Department as conflicts arise.

The L-3 Code of Ethics and Business Conduct ("Code") applies to everyone who does business on behalf of L-3 - employees, officers and members of our Board of Directors. It also may apply to agents, consultants, contract labour and others who act on L-3's behalf. Above all, every L-3 employee must conduct himself or herself in an ethical manner.

Specifically, everyone who represents L-3 will ensure that:

- ✓ Ethical behaviour is the foundation by which we conduct our business
- ✓ We do not take advantage, or abuse our position for personal gain or otherwise knowingly violate the law
- ✓ Our actions do not create, directly or indirectly, a conflict of interest
- ✓ We seek guidance when necessary

**Requirements**
If you are a U.S. citizen working outside of the United States, you are required to abide by United States laws, as well as the laws and regulations of the country in which you are employed. All other individuals may or may not be subject to both U.S. and foreign laws, depending on the circumstances.

According to the US Federal Acquisition Regulation (FAR), you are under a mandatory obligation to disclose any credible evidence of US federal criminal law violations involving fraud, conflicts of interest, bribery or violations of the gratuity regulations, as well as claims under the Civil False Claims Act, and significant overpayments. This mandatory disclosure obligation lasts for up to three (3) years after contract close-out. Due to this mandatory disclosure obligation, all L-3 employees must immediately report any issues that could constitute a violation of criminal or civil law, or a significant overpayment on a Government contract or subcontract, to your responsible Ethics Officer or the Corporate Ethics Officer. You may also report such issues through the Helpline (cf. p. 26). You are under a mandatory obligation to report such issues, but you may use the Helpline if you prefer to remain anonymous.

In situations where you are uncertain about whether a particular law applies, consult with your Manager or the Legal Department immediately.

Below are some laws particularly applicable to doing business in Norway:

- The Criminal Code §§ 270-276c
- The Company Act §§ 6-17, 6-27 and 6-28
- The Act on Securities Trading
- The Marketing Act §§ 28 and 29
- The Personal Data Act with Regulations
- The Working Environment Act
- The Internal Control Regulation re. Systematic Health, Environmental and Safety Activities in Enterprises

These laws are generally consistent with the Code and complement it. An exception is the Personal Data Act with Regulations, which modifies the Code's provisions on protecting privacy, as follows:

**Protecting Privacy**
The Norwegian Personal Data Act, with Regulations, sets out certain conditions with regard to the employer's opportunity to monitor and access an employee's e-mail and other information systems, in addition to the L-3 Code of Ethics and Business Conduct. The international L-3 Code of Ethics and Business Conduct paragraphs on Protecting Privacy (p. 14) and Use of Information System Assets (p. 17) should therefore be read with the following amendment:

An employer may only monitor and access e-mail and other information systems belonging to an employee, including his personal area of the company data network and other electronic equipment,on the conditions set out in the chapter 9 of the Norwegian Personal Data Regulation, which briefly can be summarized as follows:

Access may be carried out:

- when it is necessary to ensure the daily business and other legitimate interests; or
- if there is substantial suspicion of gross breach of the employee's duty or grounds that may result in dismissal with notice or summary dismissal.

Any monitoring and accessing of the employee's e-mail and other sources of information by the Company shall be documented. The employee shall, as a main rule, be informed in advance, as well as be given the opportunity to be present when his/her e-mail and other sources of information are accessed.