Space Systems/Loral, LLC
CODE OF CONDUCT AND BUSINESS ETHICS

Effective Date: March 28, 2017

CONTENTS

CODE OF CONDUCT AND BUSINESS ETHICS

I. PURPOSE AND SCOPE OF THE CODE

A. Statement of our Commitment and Purpose of the Code — Why do we have a code of conduct?

Space Systems/Loral and its Subsidiaries ("SSL" or the "Company") is committed to conducting business ethically, legally and consistent with our core values. Those values encourage us to treat our fellow employees, customers, business partners (vendors, suppliers, consultants) and communities with respect, fairness, honesty, trust and integrity. As SSL employees, we are all expected to adhere to the highest ethical standards of conduct, perform our work with excellence, comply with all SSL policies and procedures and comply with the spirit and letter of all applicable laws and regulations. This is important in our dealings with commercial companies as well as with the United States and foreign governments. The purpose of this Code of Conduct and Business Ethics (the "Code") is to provide a common set of ethical principles and standards to guide our actions as we conduct our business and to serve as a resource for all of us.

This Code applies to all employees of SSL company-wide in all locations, both domestic and international. This Code allows each of us—directors, officers, employees, consultants, contingent and temporary workers and interns—to know what is expected of us, regardless of role, culture, education or background. Because we want our customers and business providers to understand how we do business and what they can expect of us, this Code appears on the SSL Web Site.

Improper activities, or even the appearance of impropriety, could result in serious adverse consequences to the Company and the employees involved in such activities. For this reason, an employee's adherence to this policy is a significant indicator of the individual's judgment and competence, and will be taken into consideration when evaluating future assignments and promotions. Insensitivity to, or disregard for, the principles set forth in this Code is grounds for appropriate disciplinary action, which may include dismissal.

B. Additional Responsibilities of Managers — Set the tone at the top

In addition to following the guidance provided in this Code, those who lead others have special responsibilities. Through their words and actions, SSL leaders must demonstrate ethical behavior by example. Leaders should emphasize the importance of acting legally and ethically, and must make it clear that business results are never more important than ethical business conduct. A leader is responsible for creating an open and supportive environment where employees feel comfortable asking questions and raising concerns.

Leaders must also ensure that the people they supervise have appropriate knowledge, training, resources, and support to adhere to SSL's ethical standards and legal requirements. Additionally, leaders have an added responsibility of ensuring their team members' compliance with the Code and to support employees who in good faith come forward to raise questions or report concerns about legal or ethical compliance or other possible violations of this Code.

C. Policies and Procedures — What else applies?

The Code is the primary reference guide regarding business practices and compliance requirements, but it is not the only resource that provides guidance. We have adopted specific policies and procedures to implement certain provisions addressed in this Code and further guide business conduct, such as the SSL policies and procedures. All of our policies are available online at SSL Web.

D. Asking Questions

This Code addresses a wide range of ethical and business principles and practices. It cannot address every issue or circumstance where ethical standards or good business conduct may be challenged or questioned; it provides the basic principles and guidance needed in order for you to conduct yourself accordingly. We encourage your questions. If you are confronted with an issue not addressed in the Code, never hesitate to ask questions or seek advice from your leader, Human Resources or the Legal Department. And, you may always contact the Ethics Hotline to report issues of concern at 1.888.772.8798 or online at www.tnwinc.com/mda.

E. Ethics Hotline and Confidential Reporting

We have established an Ethics Hotline that can be called toll-free at any time (24 hours a day, 7 days a week) from anywhere in the world where we do business. The number is 1.888.772.8798 or online at www.tnwinc.com/mda. Reports to the Ethics Hotline may be made anonymously although providing your name and contact number will enable the Company to contact you during the course of the investigation if needed. SSL will protect your identity whenever possible and will respond to any perceived or actual act of retaliation experienced by anyone who reports an issue in good faith. You may also contact the VP for Legal or the VP for Human Resources at 3825 Fabian Way, Palo Alto, CA 94303.

F. No Retaliation

SSL prohibits retaliation against employees who, in good faith, submit a complaint or participate in the investigation of any complaints. If you believe that you or others are the subject of retaliation for reporting or participating in an investigation, you must report the matter to Human Resources or the Legal Department so that we can take appropriate action.

We will not tolerate retaliation so we take claims of retaliation extremely seriously. SSL also prohibits retaliation against an employee's family member.

No policy in this Code should be read to preclude you from exercising your rights under the law, from discussing terms and conditions of employment or from reporting fraud or violations of law to any governmental agency or law enforcement agency.

II. STANDARDS FOR ETHICAL AND BUSINESS CONDUCT

A. Integrity in SSL Relationships

1. Marketing SSL Products and Services

As SSL employees, we may only make accurate and truthful statements when discussing our products or services in business-related conversations, advertising or other public communications. Please consult with the Legal Department if you have any questions concerning laws or regulations that might apply when marketing or discussing our products or services.

2. Quality of Products and Services

In order to ensure that SSL maintains and builds good will with our customers, we must always be sure that our products and services meet our contractual obligations and our customers' expectations.

3. Payments to Contractors

Payments to contractors must be made pursuant to the written terms of their contracts. If you have any questions about paying or entering into a contract, please consult Operating Policy J03, *Purchaser Commitments and Supplier Contacts*, and the *Approval Matrix* available online, or inquire with the Legal Department.

4. Relationships with Business Providers

You must use care and good judgment in selecting and maintaining relationships with SSL's business providers. In the selection of business providers, you must act fairly and consistently with SSL's values. You are also responsible for informing business providers of their requirement to comply with applicable SSL policies and this Code. Before entering into an agreement with a business provider, you must ensure that the agreement is in writing and, when appropriate, you must consult with the applicable SSL leader for approval as detailed in Operating Policy J03, *Approval Matrix* and *Purchaser Commitments and Supplier Contacts*, which can be found online.

5. Retaining and Dealing Fairly with Our Business Partners

Before doing business with any company, we must conduct all appropriate due diligence to ensure that the prospective business partner is competent, qualified, follows the law, and is willing to comply with applicable SSL policies.

As we expect our business partners to deal legally, ethically and fairly with us, SSL is committed to dealing legally, ethically and fairly with our business partners. When engaging, doing business with, or managing our relationships with our business partners, we must follow all applicable SSL policies and the law, and must honor our contractual obligations. Procurement decisions must be made legally, ethically and fairly, and must be based on sound business reasons such as price, quality, schedule, and suitability. Similarly, we may not discriminate in our dealing with current or prospective customers and suppliers.

B. Employment Practices

1. Equal Opportunity and Non Harassment

It is the policy of SSL to provide equal employment opportunity to all qualified applicants and employees. SSL does not make employment decisions on the basis of race, color, religious creed, sex, sexual orientation, gender, gender identity, gender expression, age, national origin, ancestry, marital status, disability, medical condition (including cancer and genetic characteristics), genetic information, military and/or veteran status, pregnancy or childbirth (or related medical conditions), citizenship, or any other basis protected by federal, state and/or local law or ordinance or regulation. SSL also provides reasonable accommodations to qualified individuals with known disabilities in accordance with applicable federal, state, and/or local law or ordinance or regulation.

The SSL equal employment opportunity policy applies to all policies and procedures relating to recruitment and hiring, training, promotion, compensation, benefits, termination and all other terms and conditions of employment. An employee or applicant who feels discriminated against should immediately notify his/her immediate manager/supervisor, the VP of Human Resources, any Human Resources Business Partner, or the Legal Department as appropriate. Inquiries or complaints will be investigated as soon as reasonably possible. Any investigation will be conducted in as confidential a manner as is consistent with the need to conduct a thorough investigation of the complaint.

Harassment of any kind of fellow employees is also prohibited and complaints of harassment should be reported to any member of SSL management or directly to the VP of Human Resources or any Human Resources Business Partner. Any complaint of harassment will be investigated as soon as reasonably possible. A complete copy of SSL's Operating Policy K09, *Workplace Harassment, and Reporting Procedures* can be found online.

SSL will not retaliate against employees who, in good faith, complain about discrimination or harassment or participate in the investigation of any such complaints.

2. Health and Safety

SSL is committed to providing a safe and healthy work environment for employees, customers and visitors. We are required to obey all safety rules, be careful at work, and immediately report any known or suspected unsafe condition to an appropriate manager. It is very important that we report any accident that causes any injury, no matter how minor it might seem at the time, so that SSL can immediately investigate the accident and comply with the law.

3. Emergency Preparation

All SSL employees should understand what to do, who to contact and where to go in the event of a workplace emergency. This means that we must all become familiar with our workplace location's evacuation procedure, and we must know whom to call to confirm we are safe or if we need assistance. Emergency Preparedness information is available online under Environmental Health & Safety *Procedure P50_9-3*.

4. Gambling, Blogging, and Solicitation and Fundraising

a) Gambling

We may not gamble or participate in games of chance, such as pools on sporting events, on company premises, on company systems, or while engaged in any business-related activity.

b) Blogging

We are also prohibited from blogging, or using message boards, chat rooms, blogs, or other community forums not related to work on company systems or during working hours. While engaging in such activity outside of work, you should at all times exercise good judgment, and remember to always maintain and protect SSL's confidential and proprietary information, and to be respectful and courteous

to fellow employees, clients or individuals who work with or on behalf of the Company. If you publish a blog, post a comment, or share an image and it has something to do with the work you do at the Company, make it clear that what you say is representative of your views and opinions and not necessarily the views and opinions of the Company.

c) Solicitation and Fundraising

To maintain a harmonious environment, SSL prohibits people who are not SSL employees from either soliciting or distributing literature in the workplace at any time for any purpose. Although SSL employees are often active and have interest in events and organizations outside of work, we may not solicit for or distribute literature about these activities during working hours or in the workplace, with the exception of Company sponsored events approved by the President such as disaster relief and holiday food and toy collections.

5. Use of Phone and E-mail Systems

SSL telephones, e-mail and computer systems are intended to be used to conduct SSL business. Although you may make limited personal calls, and may send and receive limited personal communications through SSL's email systems and use the internet, you are expected to exercise good judgment in using these systems.

As permitted by law, all telephone calls on SSL phones may be recorded or monitored, and all e-mails and other data created, stored or transmitted on or through SSL's voicemail, e-mail and computer systems are subject to access by SSL at any time and are not considered to be confidential or private. The following are specifically prohibited in electronic communications:

- Statements that violate other SSL policies, such as SSL's prohibition against discrimination and harassment or participation in impermissible or illegal activities (e.g. gambling).

- Accessing, downloading, uploading, saving or sending sexually oriented or other offensive materials.

6. Workplace Violence

All employees should feel safe and secure in a workplace free from violence and hostility. Consequently, you may not engage in behavior that may be considered threatening, hostile, or abusive in the workplace, during working hours, or while on SSL business. Additionally, you may not possess a weapon on SSL property.

7. Substance Abuse – Illegal Drugs

We are committed to establishing and maintaining a drug-free environment for our employees. You may not be under the influence of, use or possess, sell or transfer marijuana, illegal drugs, drug paraphernalia, or controlled substances that were prescribed to another individual at the workplace or while on SSL business. A complete copy of SSL's substance abuse policy can be found online at *K44, Drug and Alcohol Free Workplace*.

8. Alcohol

Except at approved SSL functions, you may not possess, be under the influence of, or drink alcoholic beverages at the workplace or while on SSL business. There are certain, limited situations where alcohol may be served at approved SSL functions with approval by a Company SVP or above, or at a business meeting. When drinking alcohol at an SSL event or while on SSL business or SSL business travel, we are all expected to do so responsibly and in moderation. A complete copy of SSL's alcohol policy can be found online at *K44, Drug and Alcohol Free Workplace*.

9. Environmental Compliance

We are committed to protecting the environment, so we are all expected to share in SSL's efforts to reduce any potential negative impact of our operations on the environment. SSL is committed to establishing and complying with "best-practice" standards for long-term sustainability, energy conservation, use of natural resources, safe management and minimization of waste, control of hazardous materials, and responsible selection of materials. This includes our commitment to follow the laws of other countries with respect to manufacture, distribution, and disposal.

C. Compliance with Applicable Laws, Rules and Regulations

We are all expected – and required – to comply with the laws, rules and regulations of the countries, states and cities in which SSL operates. Based on the many locations of SSL's business operations, it is possible that the Code or any other established policy may conflict with a specific law and/or regulation of a particular location. If such a circumstance arises, you must comply with the applicable jurisdiction's law. If an established historic practice or local business custom conflicts with the Code, you must comply with the Code.

SSL's objective is to excel as a responsible and reputable supplier to our customers. In attaining this objective, no employee shall, on behalf of SSL or while an SSL employee, engage in any conduct that violates any law or is otherwise inconsistent with the highest levels of honesty and integrity. Complex laws and regulations govern the environment in which we do business. This Code outlines key aspects of those laws and regulations as well as relevant SSL policy. However, it may not address every circumstance or detail, so if you have questions concerning laws, rules and regulations that relate to SSL's business or the Code, please consult with the Legal Department.

Some laws of particular relevance to our business include, but are not limited to:

1. Bribery, Payments to Foreign Officials and the FCPA

SSL prohibits bribery or kickbacks of any kind and to anyone in the conduct of its business. The U.S. Foreign Corrupt Practices Act (the "FCPA") governs the types of payments or gifts that can (and cannot) be made to foreign officials for business purposes. The FCPA prohibits improper payments to foreign officials in order to obtain or retain business in a foreign country. It is important to note that under the FCPA, SSL considers the employees of certain SSL customers and potential customers to be foreign officials for purposes of the FCPA as a consequence of the government investments in those entities. The Legal Department maintains a list of those customers and potential customers which are state-owned or state- controlled enterprises. While the FCPA allows certain type of business-related payments, such as "facilitating payments," the rules and interpretations concerning such payments are not intuitive. Moreover, the application of the FCPA to specific circumstances can be complex. If you are unsure of whether the FCPA applies, prior to making any payment or gift to any foreign official, you should consult with the Legal Department. Greater detail in this respect is included in Operating Policy L23, *Compliance with the Foreign Corrupt Practices Act*, available online.

2. Money Laundering and the USA PATRIOT Act

Money laundering is a criminal activity in which the proceeds of a crime are hidden or converted in some way to make them appear legitimate. SSL is committed to complying with international laws and regulations regarding money laundering and terrorist financing, including relevant provisions of the USA PATRIOT Act in the United States and similar legislations in other countries.

3. Currency Laws

SSL conducts business in a number of foreign jurisdictions. It is our responsibility to ensure that all transactions comply with foreign exchange rules, as well as local currency laws and exchange rules.

4. Economic Sanctions

The Treasury Department's Office of Foreign Assets Control ("OFAC") administers United States economic sanctions against foreign countries, entities and individuals to counter external threats to the United States national security, foreign policy or economy. SSL and all of its employees must comply with the more than 20 OFAC-administered sanctions programs. This includes complying scrupulously with the conditions, limitations, provisos, requirements and terms of all "specific licenses" issued to SSL by OFAC and of all "general licenses" issued by OFAC in connection with any export, import, re-export, transfer, sale, marketing activity or proposal by SSL. Violations of United States economic sanctions may result in the imposition of civil or criminal penalties on individuals and, in certain cases, the entity for whom they act. Any employee who violates United States economics sanctions (or causes the Company to violate such sanctions) is subject to disciplinary action, potentially including termination of employment, in addition to any civil and/or criminal penalties imposed by the United States government. Greater detail in this respect is included in Operating Policy L04, *Compliance with U.S. Sanctions (OFAC)*, available online.

5. Export Control Laws

The Company complies, and all of its employees are required to comply with United States export control laws and regulations, including the Arms Export Control Act ("AECA") and International Traffic in Arms Regulations ("ITAR"); the Export Administration Act ("EAA") and Export Administration Regulations ("EAR"); embargo and trade sanctions laws and regulations; Anti-Boycott laws and regulations and Executive Orders pertaining to U.S. export control laws and regulations.

Many of the Company's products (hardware, software, technology and technical data) and activities (including certain marketing activities and proposals) are "controlled items" under the EAR or "defense articles" and "defense services" under the ITAR. Employees should be aware that an export occurs under the EAR or ITAR by sending or taking a controlled item or defense article out of the United States in any manner; disclosing (i.e. oral or visual disclosure) or transferring technology or technical data to a foreign person, whether in the United States or abroad; performing a defense service on behalf of, or for the benefit of, a foreign person, whether in the United States or

abroad; disclosing or transferring in the United States any defense article to an embassy, or any agency or subdivision of a foreign government; or transferring registration, control or ownership to a foreign person of any satellite.

The export of controlled items or defense articles and defense services requires the prior authorization of the United States government (Commerce Department for EAR exports or Department of State for ITAR exports) unless a specific United States government statute applies.

SSL must comply scrupulously with the conditions, limitations, provisos, requirements and terms of all licenses and other United States government authorizations (including, without limitation, export licenses, exemptions, exceptions, technical assistance agreements and manufacturing licensing agreements) in connection with any export, import, re-export, transfer, sale, marketing activity or proposal by the Company.

Failure to comply with United States export control laws and regulations, or any licenses or other United States government authorizations, can result in severe penalties for the Company and the individuals involved. Any employee who violates export control requirements may be subject to disciplinary action, potentially including termination of employment, and may be subject to civil and/or criminal penalties imposed by the United States government.

Greater detail in this respect is included in Operating Policy EC01, *Export Compliance and Licensing*, available online.

6. Competition, Fair Dealing and Intellectual Property Rights of Third Parties

SSL is committed to excelling in its industry, and seeks to achieve that goal fairly and honestly. SSL is committed to complying with applicable antitrust and competition laws. Although we recognize the importance of competition, we may not adopt unethical, unfair, or illegal business practices. We respect the rights of, and conduct business fairly with, customers, suppliers, contractors, and competitors. We should not unfairly take advantage of anyone by way of manipulations, misrepresentation of material facts, concealment, abuse of privileged information, misuse of copyrighted information or other intellectual property rights or any other illegal trade practice. Stealing proprietary information of any form, possessing trade secret information that was obtained without the owner's consent or inducing such disclosures by past or present employees of other companies is prohibited. If you are unsure whether specific activities constitute unfair business practices, please consult with the Legal Department. Additionally, Operating Policy L03, *Antitrust Compliance*, is available online and contains more, detailed guidance on competition and fair dealings.

a. Gathering Information About Competitors

While being aware of and gathering available information about competitors is often an important part of successful business operations, in doing so, we must avoid the appearance of impropriety and must not engage in illegal, deceptive or unfair means. For example, we may not steal proprietary information, observe it under false pretenses, possess trade secret information that was obtained without the owner's consent or induce such disclosures by past or present employees of other companies.

b. Statements About Competitors

We are expected to promote SSL, its services, and its products ethically and fairly, and we may not make unfair, misleading or inaccurate representations about our competitors, their services or their products or comment on their character or financial condition.

c. Standards Organizations and Other Organizations Involving Competitors

We may participate in standards organizations and industry associations, provided there is no discussion of prices, sales terms, market-divisions or similar topics.

7. Cooperation with Internal and External Investigations

Occasionally, SSL will conduct or participate in an internal or external investigation. When this occurs, we are all required to cooperate fully with these investigations if requested to do so. Our responsibility to cooperate with these investigations remains even after the end of our employment with SSL.

Additionally, you must notify the Legal Department of any government inquiry, court order or legal proceeding about which you become aware. You should do this before responding to such inquiry, order or proceeding.

SSL will maintain the appropriate level of internal investigations' confidentiality. If you are participating in an investigation, you should never discuss its existence subject matter or facts with anyone other than the individual leading the investigation unless authorized or legally required to do so.

Please also keep in mind that SSL has the discretion to search without notice work areas, computers and personal belongings, and that you are required to cooperate with any requested search. If you have any questions or concerns, please contact the Legal Department.

8. Acting or Speaking on Behalf of SSL

Our authority to act on behalf of SSL is limited by various laws, regulations, and internal policies. We may not sign documents or otherwise represent or exercise authority on behalf of SSL unless specifically authorized to do so. Consequently, you should be aware of situations in which you might be perceived as representing or speaking on behalf of SSL, especially in public communications (blogs, etc.). You should not make any statements on behalf of SSL unless it is a part of your job or unless you are specifically authorized to so. Any public speaking engagement or publications relating to SSL must be pre-approved by the Marketing department.

9. Relationships with Affiliates

All transactions between and among SSL's affiliates must comply with applicable laws, regulations and SSL policy.

III. CONFIDENTIAL AND PROPRIETARY INFORMATION

A. SSL Information

SSL's information, data, and related resources have been developed at great expense and effort. We must all maintain the confidentiality of SSL information that has been entrusted to us by SSL, our customers or our suppliers, and we may not use this information for our personal advantage or disclose it to third parties absent an appropriate agreement. We should take precautions to make sure such information is secure by, for example, avoiding discussing confidential information in public areas. In conversations with our customers and suppliers, we should take care to disclose only information which they have a legitimate need to know.

Confidential and proprietary information includes, but is not limited to:

- SSL research and development, such as inventions, patent applications, and engineering and laboratory notebooks (see below);
- Customer and employee records;
- Business strategies, business results, unannounced products or services, marketing plans, pricing and financial data;
- Non-public information about products or services, including hardware and software specifications and designs;
- Confidential organizational information; and
- Information disclosed by other parties pursuant to a non-disclosure agreement.

Confidential and proprietary information may exist as reports, manuals, charts, computer disks, drawings, specifications, photographs, films, and correspondence. Hardware, equipment, or materials embodying proprietary information and data may also be treated as proprietary information.

There are certain situations where disclosure of confidential information is permitted or legally required. Moreover, nothing in this Code prohibits or restricts you from initiating communications directly with, responding to any inquiry from, or providing information to or testimony before, the Securities and Exchange Commission, Department of Justice, or any other governmental agency or self-regulatory organization, about actual or potential violations of laws or regulations. You are not required to obtain SSL's prior authorization before engaging in such communications, nor are you required to inform SSL about such communications.

As a general rule, please keep in mind that SSL information includes all non-public information that, if disclosed, might be of use to competitors or harmful to SSL, its customers or suppliers. For additional guidance, please refer to Operating Policy L02, *Release of Information to the Public*, and A27, *Safeguarding Proprietary Information*.

It is important to remember that our obligation to preserve and not reveal confidential information continues even after the end of the employment relationship.

B. Employee, Customer and Supplier Information

In addition to protecting SSL's information, we must also protect our customers' and suppliers' confidential information. Accordingly, we may not use, access or disclose customer or supplier information unless we are specifically authorized to do so or we are required to do so in order to comply with the law. For additional guidance, please refer to Operating Policy A53, *Safeguarding Customer Proprietary Information*, available online.

Data Privacy Legislation: Many countries have strict data privacy and protection laws for data relating to employees and customers. We should respect these laws, which restrict the processing, retention or transfer, among other things, of "personal data". If you have any questions regarding these laws, please consult with the Legal Department.

C. Confidential Prior Employer or Competitor Information

We may not solicit confidential information from anyone currently or formerly employed by competitors, nor accept the confidential information of others without the written consent of the rightful owners of such information. Likewise, SSL respects the confidentiality requirements of prior employers. Employees are not expected to disclose to SSL or induce SSL to use any confidential or proprietary information or material belonging to any previous employer or anyone else.

IV. PROTECTING SSL'S ASSETS AND REPUTATION

A. SSL Assets

As SSL employees, we are required to protect, properly maintain and safeguard from theft, waste, carelessness or misuse, all SSL assets. These assets include financial assets, physical assets such as equipment and supplies, customer relationships, and intellectual property, such as information about products, services, customers, systems, computer programs and software, and people.

All property created or obtained by SSL belongs to SSL, and may only be used for the conduct of SSL business (except where incidental use is permitted, such as when making limited personal phone calls). We may not use SSL's assets for personal gain, and we are required to return all SSL assets at the conclusion of our employment relationship.

B. Intellectual Property

We are all responsible for establishing, maintaining, and protecting SSL's rights in its intellectual property. In this regard, we are required to cooperate fully with SSL's efforts to patent, register, or otherwise protect its ownership interests in its intellectual property. Generally, "intellectual property" includes any information, discovery, development, concept, idea, process, or work related to SSL's business, written or otherwise, whether or not it can be patented or copyrighted, that is developed alone or with others during employment with SSL. Additionally, it is SSL's policy to respect the intellectual property rights of others. Please consult with the Legal Department if you have any questions.

C. Protecting SSL and Software Piracy

We must all take reasonable steps to protect the security of any password or access number we use in connection with any SSL computer, network or communication device. Before installing any electronic media (software, diskettes, CD-ROMs, and file) acquired through public networks, such as the Internet, we must first check them for viruses.

D. Software Piracy

We may only use approved and properly licensed software on SSL systems, and may only use appropriate software in accordance with the applicable software owner's licensing agreements. Additionally, we may not make an unauthorized copy of any software that may be either licensed to or owned by SSL.

E. Sabotage and Espionage

We are all expected to secure SSL property, including SSL systems, SSL information and SSL premises, from sabotage and espionage. This means that you should not leave visitors unattended or sensitive areas unsecured. Above all, please use your common sense and immediately report any suspicious activity.

F. Misuse of Company Benefits

We provide a variety of benefits to our employees. You must use SSL benefits for the purpose they were provided.

G. Proper and Timely Reporting of Public Documents

As a public company, it is of critical importance that SSL's filings with, and submissions to, government entities and regulators, and other public communications, be fair, accurate and timely. Depending on his or her position with SSL, an employee may be called upon to provide necessary information to assure that SSL's public reports are complete, fair and understandable. SSL employees are expected to take this responsibility seriously and to provide prompt and accurate answers to inquiries related to SSL's public disclosure requirements.

H. Internal Controls

SSL has a detailed financial control structure and related procedures designed in accordance with securities regulations which require companies to implement and evaluate internal controls for purposes of financial statement reporting integrity. Assessing the quality of these internal controls involves a continuous process of evaluating their design and operation and taking necessary corrective action to improve them as required. Through discussions with managers and review of SSL's documented practices and procedures, each employee must understand his or her role with regard to SSL's overall control structure and related procedures. An employee should report as soon as possible to his or her manager or other appropriate person in accordance with Section VIII of this Code any potential concerns he or she may have with respect to either his or her own role or performance or otherwise relating to SSL's control structure and related procedures. Early identification of problems is critical to the strength of the Company's controls, as well as maintaining compliance with the law.

I. Record Keeping

We are committed to maintaining and providing truthful information that fully satisfies applicable legal requirements. Various laws and accounting standards govern our record keeping and information disclosures. We all must create accurate records that reflect the true nature of the transactions and the activities that they record. Our records must

be full, fair, timely, accurate, and understandable. You must resolve discrepancies in any records and make appropriate corrections. If you are unsure about the proper accounting treatment of a financial transaction, please consult with the Corporate Controller for guidance. Employee records such as for time, work and absence must also be accurately and completely recorded.

To ensure only relevant and accurate documentation is retained, if you are directly involved in the preparation and review of financial records, you should follow SSL's Operating Policy A06, *Document Management System (Records Retention)*, available online. You may never destroy, alter, mutilate, or conceal any record if you have been directed to retain it or if you know—or contemplate or reasonably believe there is a possibility—of any litigation or internal or external investigation concerning the subject of that record.

J. Legal Hold/Document Preservation Policy

Any and all records that may reasonably be used in or may reasonably be relevant to an actual, pending or reasonably anticipated legal proceeding, or internal or external investigation ("Legal Proceeding") must be carefully preserved and maintained for the duration of the Legal Proceeding or the time period set forth in any "Litigation Hold" or "Preservation Notice" distributed in connection with any Legal Proceeding, in addition to any retention period set forth in the applicable records retention policy. You must consult with the Legal Department before disposing of any records relating to a Legal Proceeding.

K. Fraudulent Behaviors and Activities

SSL employees may not engage in, or attempt to encourage or influence others to engage in, illegal or fraudulent behaviors or activities. Such activities include those specifically prohibited in this Code, as well as any other dishonest act, whether performed intentionally or unintentionally. In addition, we are required to report to the Legal Department known or suspected incidents of fraudulent or illegal activities. Please consult with the Legal Department if you have any questions about what constitutes a fraudulent or illegal activity.

L. Following Security Guidelines

While SSL's customer base is now primarily commercial companies, SSL continues to contract with the United States government or its prime contractors. These contracts require the Company to implement and maintain a system of security controls. As SSL employees, we all are individually responsible for safeguarding classified information. The following are some of the key rules that employees must follow:

- Wear your badge prominently.
- Notify your manager of any circumstances that might embarrass or damage the Company.
- Establish a system to ensure that unattended classified files are always locked.
- Safeguard and transmit all classified material in accordance with government and SSL requirements.

You are also prohibited from sending classified information via regular mail. Additionally, you should never discuss classified information, company plans or related information with family, friends, or other unauthorized persons. Any and all classified activities must be conducted on US Government approved telephonic and IT systems/networks in approved spaces/facilities only by SSL employees with the appropriate security clearance and with a valid need to know. Classified conversations are never permitted outside of these spaces and on any unclassified telephonic, cellular or IT system/network.

You should be particularly careful when using phones of any type, especially cellular phones, for sensitive or classified conversations. This also applies to use of computer terminals, facsimile machines, cellphone cameras and other equipment used to transmit information or data. Finally, only authorized personnel are allowed to use a camera within SSL facilities. Such usage shall be in accordance with SSL's *Camera Policy*. A complete copy of SSL's Operating Policy A51, *Camera Usage at Space Systems/Loral*, can be found online.

If you have any questions about security matters, contact your immediate manager, security representative or Tim Perry, Corporate Director of Security, at (650) 852-4345. A complete copy of SSL's Operating Policy SEC01, Security, can be found online.

V. CONFLICTS OF INTEREST

We all have a responsibility to avoid situations or circumstances where a conflict of interest might occur or appear to occur. Generally, conflicts of interest are situations, arrangements or circumstances where one's private interests interfere (or appear to interfere) in any way with SSL's interests. For example, an actual or potential conflict of interest occurs when an employee is in a position to influence a decision or have business dealings on behalf of SSL that might result in a personal gain for the employee, or for the employee's relatives or colleagues. We are required to disclose potential conflicts so that SSL may assess and prevent conflicts of interest from arising, and protect everyone involved. If you have questions regarding potential conflicts of interest, please consult with the Legal Department.

A. Personal Relationships

1. Conducting Business

We should avoid conducting SSL business with family members or with family-controlled businesses. If this is unavoidable, we may not give the related party preferential treatment. Our direct family members should also comply with this policy. And as noted above, since we are required to disclose potential conflicts, we should inform SSL whenever there is a possibility that we may conduct business with a family member or a family-controlled business.

2. Hiring, Supervision and Evaluation

Unless prohibited by law, we may not hire, supervise, or participate in the evaluation process of any individual with whom we share a personal or familial relationship unless explicitly authorized to do so. We understand that employees may establish dating relationships with co-workers. Employees are expected to exercise good judgment in pursuing romantic relationships in the workplace and recognize that relationships between co-workers can, depending upon the work roles and respective positions of the dating co-workers, create an actual or apparent conflict. Employees must promptly disclose the existence of a romantic relationship with another SSL employee or contractor to Human Resources.

B. Outside Employment, Directorships, Business Interests and Political Activities

1. Outside Employment

We may pursue outside interests as long as we can satisfactorily perform our SSL job duties, and the outside interests do not interfere with SSL scheduling demands or conflict with SSL's business. However, we may not perform any services for customers on nonworking time that are normally performed by SSL personnel. Additionally, we may not solicit or conduct any outside business while at the SSL

workplace or during scheduled SSL working hours. We may not be simultaneously employed by a supplier, customer, or competitor of SSL. We are committed to advancing SSL's interests and should do so whenever possible.

SSL employees may not, without being granted an exception, acquire or retain, either directly or indirectly, the following financial interests in an organization that competes with, does business with, or seeks to do business with SSL:

- Any interest as a proprietor or partner in such an organization;
  - The ownership of, or right to acquire, stock or bonds of such an organization that is a privately held corporation; or
  - With respect to a publicly-owned corporation five percent (5%) or more of the revenues of which are derived from SSL, the ownership of, or right to acquire, stock or bonds in an amount in excess of the lesser of (i) $25,000 or (ii) 1% of the total securities of such publicly owned corporation.*

Each employee shall report to the SSL President the details on any of the financial interests described above that are held or acquired, directly or indirectly, by himself or herself or any family member, to the extent known by the employee.

If you believe an outside employment may result in a conflict of interest, you must obtain prior written approval from the SSL President. If you choose to pursue outside employment, you must also disclose its nature and/or scope to your supervisor or manager.

2. Outside Directorships

You may not serve as an officer or director of any firm without prior approval by the president of SSL.

3. Outside Business Interests

Because certain outside business interest or our investments in the business interests of customers, suppliers, and competitors have the potential to compromise our responsibilities to SSL, they must follow SSL policies regarding ethical business practices, confidentiality and conflicts of interest. If you have any questions or concerns about such outside business interests, please consult with the Legal Department before engaging in such matters or making such investments.

4. Political Activities

We must keep our personal political contributions and interests separate from our activities with SSL. Under no circumstances may we pressure our colleagues to make political contributions or participate in, or support, a political campaign. If you wish to volunteer for a political campaign, you may do so, but on your own

time and not in connection with your employment with SSL.

In addition, you have the right to participate in the political process and make personal contributions to a political campaign from your personal funds. However, unless required by law, when making political contributions, you may not refer in any way to your employment with SSL.

If you intend to seek a political office, please consult with, and obtain approval from, the Legal Department to avoid conflicts of interest.

5. Charitable Activities in SSL's Name

It is an important value of SSL to improve the quality of life in our communities. SSL encourages us all as private citizens to engage in community service and contribute to community programs. SSL regularly participates in and conducts various charitable and community support programs in SSL's name, such as food and toy drives during the holidays and the United Way. If you would like to participate in or conduct such charitable activities in SSL's name, you must first obtain approval from Human Resources.

[*]This restriction does not apply to employees who come to SSL from other companies and who hold shares of those companies' stock in a savings plan or stock ownership plan. This exception only applies to stock that was owned by the employee prior to his or her employment with SSL, and that is held in those investment instruments. Subject to the terms of the plan document, such employees may keep stock that is in those investment instruments and any stock dividends paid from those remaining in those investment instruments.

C. Gifts

1. Payments or Gifts from Others

We should avoid any implication that preferential treatment will be granted or received in our dealings on behalf of SSL. Occasionally, outsiders such as suppliers or contractors may make payments or give gifts to us. Under no circumstance should we accept payments. Although we may never solicit gifts or anything of value from individuals or corporations that might do business with SSL, we may accept gifts that are fair and free of improprieties, provided the gift does not exceed USD $250 in value. In certain circumstances, local customs may require that more valuable gifts be exchanged. While SSL strives to respect local customs, gifts of this nature may not be exchanged without prior approval of the SSL President or Legal Department. As a general rule, all gifts received should always be appropriate under the circumstances, and should never be of a kind that could create an appearance of impropriety.

Returning Gifts: If a gift exceeds the monetary value provided in this Code, or if it in any other way is inappropriate or violates SSL policy, you should return the gift with an explanation that SSL policy does not permit you to accept it. If the gift is perishable and its return is not practical, you may either donate it anonymously to charity or share it with your colleagues (provided that the shared portion of the gift does not exceed the $250 limit). If you have any questions regarding the return of a gift, including situations where the return of a gift is impossible, please consult with the Legal Department.

2. Providing Gifts, Meals or Entertainment

The purpose of providing gifts, meals and entertainment is to promote goodwill in our working relationships. Business-related gifts not prohibited by law (such as the FCPA) should be reasonable and customary in the context of the relationship with the recipient of the gift, appropriate for the occasion, and in accordance with SSL policies. If you have any questions about providing gifts, meals or entertainment, please consult with your manager or the Legal Department.

D. Corporate Opportunities

As a general rule, we may not take for ourselves personally opportunities that are discovered through our use of SSL property, information, or our position.

E. Insider Trading Policy

If you become aware of material nonpublic information relating to SSL or MDA, you may not, directly or through family members or other persons or entities: (a) buy or sell securities of MDA, or engage in any other action to take personal advantage of that

information or (b) pass that information on to others outside SSL, including family and friends. In addition, if in the course of working for SSL, you learn of material nonpublic information about a company with which SSL does business, including a customer or supplier of SSL, you may not trade in that company's securities until the information becomes public or is no longer material.

For additional, detailed guidance, please refer to the *MDA Insider Trading Policy*, which is posted online.

VI. SPECIAL REQUIREMENTS WHEN MARKETING AND CONTRACTING WITH THE FEDERAL GOVERNMENT

In dealings with the United States Government, SSL employees and other representatives who perform legislative liaison, marketing, proposal and/or contract activities should be especially sensitive to the following regulations:

A. Gifts and Gratuities to Government Personnel

The Company must comply with special standards of conduct in contracting with the federal government. Government representatives shall not be offered or given, either directly or indirectly, anything of value that they are prohibited from receiving by applicable agency regulations. SSL employees dealing with representatives of a particular federal agency are responsible for complying with that agency's standards of conduct. Where there is a question as to a particular agency's requirements under its standards of conduct, employees must contact SSL legal counsel for guidance.

Except as otherwise permitted by law or regulation, SSL employees are prohibited from paying for meals, refreshments, entertainment, travel or lodging expenses for any U.S. government employee or representative. While there is a regulatory exception under which a federal employee may receive a gift of less than $20 in value, such as a meal provided on-site to accommodate continuing business meetings, this exception is limited in nature, and in no event may that Federal employee receive more than $50 total in such gifts in a calendar year. Given the very limited nature of these exceptions, SSL employees should not offer to pay for U.S. government employee meals, provide transportation to U.S. government employees (i.e., rides in rental cars or cab sharing) or pay for entertainment for any U.S. government employee, as these types of gestures may run afoul of the gift and gratuities rules, which apply to SSL and to the U.S. government employee. Similarly, SSL employees doing business with state or local government officials are responsible for knowing and adhering to the rules that may apply to such state or local government employees.

In certain instances where customs in foreign countries require the exchange of gifts, and the intended recipient is a foreign government employee, the Company will provide the gift

after confirming that the FCPA does not prohibit such a gift or exchange. Any gifts received by any SSL employee, other than those of truly nominal value, will become Company property.

B. Lobbying the Federal Government

When engaging in lobbying activities with the federal government, SSL employees must comply with the Lobbying Disclosure Act of 1995 ("Lobbying Act"), the Byrd Amendment and related regulations. Lobbying activities are defined as any oral or written communication to certain executive and legislative officials made on behalf of a client with regard to certain federal matters and efforts in support of such communications, including preparation and planning activities, research and other background work, with some exceptions.

The Lobbying Act is primarily a registration and reporting statute, which requires lobbyists (individuals or entities) to register with Congress and to submit quarterly disclosure reports of lobbying activities and semi-annual reports of certain campaign contributions. When a company registers on behalf of its employees who are lobbyists, the company completes the required filing.

The Byrd Amendment both prohibits certain lobbying activity and requires reporting of other lobbying activity. The Byrd Amendment prohibits the use of funds received through government appropriations from being expended on certain lobbying activities. The Byrd Amendment also requires government contractors to file disclosure reports of lobbying activity to government agencies when requesting or receiving certain federal contracts, grants, loans or cooperative agreements.

Finally, certain lobbying costs are unallowable under the Federal Acquisition Regulation.

SSL employees must learn and adhere to these laws and regulations if they intend to engage in any lobbying activity with the federal government and must maintain complete and accurate records of all lobbying activity. SSL employees who intend to lobby state or local governments are responsible for knowing and adhering to the laws that may apply to such activities.

C. Restrictions on Obtaining Bid and Proposal or Source Selection Information

Federal law prohibits contractors, their employees, representatives, agents and consultants from obtaining bid and proposal or source selection information related to any federal agency procurement before award of the contract.

A contractor's bid or proposal information includes any of the following information

submitted to a federal agency in connection with a bid or proposal that has not been made available to the public:

- Cost or pricing data;
- Indirect costs and direct labor rates;
- Proprietary information;
- Information marked "contractor bid or proposal information" in accordance with applicable law or regulation or marked with any other appropriate restrictive or proprietary language under applicable laws or regulations.

Source selection information includes the following information prepared for use by a federal agency for the purpose of evaluating bids or proposals, if the information has not been publicly disclosed:

- Bid prices submitted to an agency or lists of those bid prices;
- Proposed costs or prices submitted to an agency or lists of those costs or prices;
- Source selection plans or technical evaluation plans;
- Technical evaluations, cost or price evaluations, competitive range determinations, rankings of bids, proposals or competitors or reports and evaluations of source selection panels, boards or advisory councils;
- Other information marked as "Source Selection Information" according to applicable laws and regulations.

If any doubt exists as to whether a particular piece of information can be rightfully obtained, the SSL employees or representatives who wish to obtain such information that has not been publicly released should first contact SSL's Legal Department. Further, unauthorized offers to provide proprietary or source-selection information must be refused and immediately reported to SSL legal counsel.

D. Employment Discussions and Hiring Government Personnel

SSL employees must comply with two types of restrictions in this complex area: (1) restrictions on holding employment discussions with certain government personnel; and (2) restrictions on the types of tasks or assignments that current or former government personnel can perform for a private employer.

SSL employees are prohibited from holding employment discussions with certain government personnel who are participating personally and substantially in matters that may affect the Company's financial interests, including federal procurements in which SSL is a bidder or offeror. Employment discussions include a broad range of conduct, such as e-mail correspondence, the exchange of a resume or a conversation over lunch in which the

possibility of employment is discussed. References to salary or other terms of employment are not necessary for a communication to constitute employment discussions. SSL employees must know and adhere to the relevant laws if they intend to engage in employment discussions with government personnel.

In addition, even if SSL is permitted to discuss employment with a particular government employee, certain current or former government personnel are restricted from working on certain matters or contracts on behalf of private employers. These restrictions may depend on the type of position, grade level or responsibility the government employee had while working in the government and can last for one year, two years or a lifetime.

The employment discussion and hiring restrictions for federal government personnel are complex; therefore, any questions should be presented to your supervisor or manager to obtain appropriate advice and guidance. A complete copy of SSL's Operating Policy K15, *Holding Employment Discussions With and Hiring Federal Government Personnel*, is available online.

E. Truth in Negotiations Act

All proposals submitted to the U.S government must comply with the Federal Acquisition Regulation (the "FAR") and the proposed contract requirements.

Where cost or pricing data are required to be submitted, such data must be accurate, complete and current as of the date of final agreement on price. Whether you are the contract negotiator, the cost estimator or the person responsible for furnishing the data to the cost estimator, you must ensure that the data meet these FAR requirements:

- Accurate means free from error;
- Complete data means all facts that a prudent buyer or seller would reasonably expect to have an effect on price negotiations, e.g., historic cost data, vendor quotations, "make or buy" decisions and other management decisions that could have a significant bearing on cost; and
- Current data means data that are up to date. Because many months may pass after the original proposal and price were submitted, data should be updated through the close of negotiations to ensure they are current.

If you have any questions as to whether information is cost or pricing data that must be disclosed to the government, you should seek advice from the SSL Legal Department. It is SSL's intention that all required cost or pricing information will be disclosed to the government. Falsely certifying facts or data used in government contracts, whether unintentionally or deliberately, is a violation of U.S. laws and contract requirements and may subject the Company and involved employees to criminal and civil penalties or administrative action.

F. Anti-Kickback Act

Employees and representatives must comply with this law which prohibits any individual or company from providing, attempting to provide or soliciting, accepting or attempting to accept, any kickback. "Kickback" is defined as any money, fee, commission, credit, gift, gratuity, thing of value (including money, trips, tickets, transportation, beverages and personal services) or compensation of any kind that is provided directly or indirectly to any individual or company for the purpose of improperly obtaining or rewarding favorable treatment in connection with a prime contract or subcontract/supplier relating to a prime contract.

In addition, government contracts contain one or more clauses related to the Anti- Kickback Act which requires contractors to establish and follow reasonable procedures to prevent and detect possible kickbacks, and to report possible violations when there are "reasonable grounds" to believe that a violation has occurred.

VII. IMPROPER INFLUENCE ON CONDUCT OF AUDITORS

You should not directly or indirectly take any action to mislead SSL's independent auditors for the purpose of rendering SSL's financial statements misleading. All disclosures made to our auditors and in our financial reports must be full, fair, accurate, and understandable.

VIII. REPORTING CODE VIOLATIONS

A. Duty to Report Code Violations

As SSL employees, we are required to discuss with the appropriate management, Human Resources (VP of HR or Business Partners) or Legal Department personnel any behavior, which we believe may be illegal, or in violation of the Code or any other SSL policy. Report any such concerns promptly so that SSL can take immediate and corrective actions. As discussed in more detail below, SSL maintains a strong policy against any type of retaliatory action taken against employees who report violations.

Please also keep in mind that, when reporting violations, you must take care that your

statements are thorough, accurate and honest.

B. Guidance on Reporting Code Violations

When reporting Code violations, please keep the following guidance in mind:

1. We all share the responsibility of ensuring that the code is observed and enforced. As such, we are required to report known or suspected violations of the Code to the appropriate level of management or the Ethics Hotline at 1.888.772.8798 or online at www.tnwinc.com/mda. For this purpose, the appropriate member of management may include your immediate leader; one of the business partners in Human Resources; or the Legal Department.
2. When reporting a suspected Code violation, you should be mindful of the following restrictions:
   (a) Do not contact the suspected violator directly to obtain additional information, determine facts or seek restitution;
   (b) Do not discuss the incident, facts, suspicious or allegations with any other individual except the appropriate member of management; and
   (c) Do not discuss the incident, facts, suspicions or allegations with anyone outside of SSL unless specifically directed to do so by the Legal Department.
3. When making such a report, please also keep in mind that the member of management who receives the report is required to obtain as much information about the incident as possible.

C. Confidentiality in the Reporting Process

Any reported allegations of Code violations, including allegations of harassment, discrimination and retaliation will be reviewed, and if it is determined that further inquiry is appropriate, investigated promptly, thoroughly and impartially. Although there is no guarantee of absolute confidentiality with respect to such complaints, confidentiality will be maintained where appropriate and feasible (regardless of the severity of the complaint), and to the extent permitted by law.

IX. COMPLIANCE WITH THE CODE AND AT-WILL EMPLOYMENT

We are all expected to read and comply with the Code in its entirety, and in conjunction with other SSL policies and procedures. After hire and on an annual basis, you will be asked to sign and date an acknowledgement affirming that you have read, understand, and agree to follow the Code, that you have not or are not violating any of its provisions, and that you are not aware of any unreported violations. Adherence to this Code is a significant indicator of an individual's judgment and competence, and will be taken into consideration when evaluating future assignments and promotions. Insensitivity to, or disregard for, the

principles set forth in this Code will be grounds for appropriate disciplinary action, including dismissal. You should be aware that although the Company may elect to impose formal discipline for Code violations that is less severe than termination, such as warnings or suspensions, no formal system of warnings or progressive discipline is required.

The Code is not intended to, and does not constitute a contract of continued employment, a promise of employment for a specified duration, or a guarantee of benefits or working conditions between any employee and SSL. Employment with SSL is "at-will," which means that you are free to resign at any time, with or without notice and with or without cause. Likewise, "at-will" means that SSL may terminate your employment relationship at any time, with or without notice and with or without cause.

As the standards for "best-practices" in business conduct and ethics may depend on the context and may change over time, SSL reserves the right to interpret, amend, modify, cancel or change any or all provisions of the Code at any time in its sole discretion.