Regulations for Implementing the Law of the People's Republic of China on Safeguarding State Secrets

(Adopted by the State Council on January 17, 2014; Effective March 1, 2014)

Chapter I. General Provisions

Article 1. These Regulations are formulated in accordance with the provisions of the Law of the People's Republic of China on Safeguarding State Secrets (hereafter referred to as the "**State Secrets Law**").

Article 2. The national secrecy administrative department shall be responsible for secrecy work throughout the country. The local secrecy administrative departments at and above the county level shall be responsible for the secrecy work within their respective administrative regions, under the guidance of the secrecy administrative departments at the higher level.

Article 3. A central state organ shall, within its scope of authority, manage or guide the secrecy work within its system, supervise the enforcement of secrecy laws and regulations and may, based on actual circumstances, formulate or together with relevant departments formulate secrecy provisions relating to the business of which they are in charge.

Article 4. The people's governments at or above the county level should strengthen their infrastructure facilities for secrecy work and the deployment of key secrecy protection technology products.

The secrecy administrative departments at or above the county level should strengthen their research and development relating to key secrecy protection technology products.

The expenses needed to fulfill the responsibilities of the secrecy administrative departments should be included in the budget of the people's governments at the same level. The expenses needed by organs and entities for carrying out their secrecy work should be included in the annual budgets or the annual plans for revenues and expenditures of those organs and entities.

Article 5. An organ or entity may not designate as state secrets matters that should be disclosed to the public in accordance with the law, nor may it disclose information involving state secrets.

Article 6. Organs and entities shall implement a secrecy work responsibility system. The responsible person(s) of an organ or entity shall be responsible for the secrecy work of that organ or entity. The staff members shall be responsible for the secrecy work at their posts.

An organ or entity should, based on the requirements of its secrecy work, establish a secrecy work office or assign personnel especially to be in charge of secrecy work.

The performance of the secrecy work responsibility system should be incorporated into the contents of the annual performance evaluation and assessments of the respective organs, entities and their personnel.

Article 7. All levels of secrecy administrative departments should organize and carry out regular publicity and education. Organs and entities should periodically implement education and training for their own personnel on such aspects as the secrecy situation, secrecy laws and regulations, and secrecy technologies and precautions.

Chapter II. Scope and Classification Levels of State Secrets

Article 8. The specific scope of state secrets and scope of each classification level (hereafter referred to as the "**scope of classified matters**") should clearly stipulate the specific titles, classification levels, secrecy periods and scope of access of the state secrets.

The scope of classified matters should be adjusted in a timely manner in light of changes of circumstances. When formulating or revising the scope of classified matters, sufficient substantiation) should be conducted to listen to opinions of the relevant organs and entities and of experts in relevant fields.

Article 9. The person in charge of an organ or entity shall be the **state secret classifier** of that organ or entity and, based on work requirements, may designate other personnel as state secret classifiers.

Personnel who are especially responsible for classification work should be subject to secrecy training, be familiar with classification duties and the scope of classified matters, and know the procedures and measures for state secret classification.

Article 10. The state secret classifiers shall, within the scope of their responsibility, be responsible for the work concerning the determination, modification and declassification of state secrets. Their specific responsibilities are:

1. To review and approve the classification levels, secrecy periods and access scope of the state secrets originated in their respective organs or entities;
2. To conduct reviews of state secrets originated in their organs or entities that are currently still within their secrecy period, and make decisions on whether to change or declassify their secrecy status; and
3. To propose preliminary classification levels for matters where it is not clear whether they are state secrets and should have what classification level, and submit such proposed designations in accordance with stipulated procedures to the secrecy administrative departments for determination.

Article 11. Central state organs, provincial level organs and organs of municipalities divided into districts and autonomous prefectures may, based on work requirements or the application of a relevant organ or entity, and within the classification authority stipulated by the national secrecy administrative department, make a delegation of classification authority within the scope of their authority.

Classification authorizations should be made in written form. The authorizing organ should supervise the authorized organs or entities on their performance in fulfilling the classification authorization.

The authorizations made by central state organs and provincial level organs shall be reported for the record to the national secrecy administrative department; the authorizations made by organs of municipalities divided into districts and autonomous prefectures shall be reported for the record to the secrecy administrative departments of the respective provinces, autonomous regions or municipalities directly under the Central Government.

Article 12. When originating state secrets, the organs or entities should make sure that persons originating the state secrets shall propose, pursuant to the relevant scope of the classified matters, the secrecy classification level, secrecy period and access scope, submit them to the state secrets classifiers for review and approval, and adopt appropriate secrecy protection measures.

Article 13. Organs and entities should with respect to state secrets they originate determine the specific secrecy period according to the provisions on the scope of the classified matter; when there is no stipulated specific secrecy period for the scope of a classified matter, the organ or entity concerned may, based on work requirements, determine it within the statutory limits on secrecy periods. Where it is impossible to determine the secrecy period, the conditions for declassification should be determined.

The secrecy period of a state secret shall be calculated starting from the date marked on which the state secret originated; where it is impossible to mark the date on which the state secret originated, the organ or entity determining the state secret should notify in writing all the organs, entities and personnel within the access scope, and the secrecy period shall be calculated starting from the date of notification.

Article 14. Organs and entities should strictly minimize the access scope of state secrets in accordance with the provisions of the State Secrets Law. A written record of personnel with access to state secrets at the secret level and above should be made.

Article 15. State secret carriers and the obvious parts of equipment and products that are state secrets should be marked with a state secrets label. The state secrets label should indicate the classification level and the secrecy period. When the classification level and secrecy period are modified, the original state secrets label should be modified promptly.

If it is impossible to apply a state secrets label, the organ or entity that determined that state secret should notify in writing the organs, entities and personnel within the access scope of that state secret.

Article 16. If organs and entities believe state secrets they originated should be declassified or their secrecy period extended pursuant to the provisions of the State Secrets Law, they should promptly be declassified or have their secrecy periods extended.

Organs and entities that believe state secrets they did not originate should be declassified or their secrecy period extended pursuant to the provisions of the State Secrets Law may submit a suggestion to the organ or entity that originally determined that state secret, or to its higher level organ or entity.

The organs or entities that originally classified archives of state secrets that have already been transferred to the state archives bureaus at various levels in accordance with the law shall conduct declassification reviews in accordance with relevant provisions of the State.

Article 17. Where organs or entities are eliminated or merged, modification or declassifications of the state secrets classified by them shall be the responsibility of the organs or entities assuming their functions. The responsibility may also go to organs or entities designated by their higher level organs or entities, or by the secrecy administrative departments.

Article 18. When an organ or entity discovers that a determination, modification or declassification by them is not appropriate, it should promptly correct it. When a higher level organ or entity discovers that a determination, modification or declassification by an organ or entity at a lower level is not appropriate, it should promptly notify the organ or entity to correct the situation and may also directly correct the situation itself.

Article 19. When dealing with an uncertain matter that is subject to the provisions of the State Secrets Law but is not clearly provided for in the scope of classified matters, an organ or entity should propose a preliminary classification level, secrecy period and access scope for it, adopt appropriate secrecy protection measures, and submit an application to the relevant departments for determination within 10 days of the day the classification level is proposed for the matter. A matter proposed to be classified as top secret or a matter proposed to be classified by a central state organ as secret or confidential shall be reported to the national secrecy administrative department for determination; and a matter proposed to be classified as secret or confidential by other organs or entities shall be reported for determination to secrecy administrative departments of the relevant province, autonomous region or municipality directly under the Central Government.

The secrecy administrative departments should make a decision within 10 days of receipt of the reports. The secrecy administrative departments of the relevant provinces, autonomous regions or municipalities directly under the Central Government should further promptly file their decisions on uncertain matters with the national secrecy administrative department for the record.

Article 20. Where an organ or entity has a different view on whether a certain classified matter is a state secret or concerning what is the appropriate classification level, it may raise its objection to the organ or entity that was the original classifier, and the original classifying organ or entity shall make a decision.

When the original classifying organ or entity fails to handle the matter or the organ or entity still objects to the decision by the original classifying organ or entity, the matter shall be handled pursuant to the following provisions:

1. Matters classified as top secret or matters classified by central state organs as secret or confidential shall be reported for determination to the national secrecy administrative department.
2. Matters classified by other organs or entities as secret or confidential shall be reported for determination to the secrecy administrative departments of the relevant provinces, autonomous regions or municipalities directly under the Central Government.

Pending a decision by the original classifying organ or entity, or a decision by the secrecy administrative department, the matter at issue should be subject to secrecy protective measures corresponding to the highest classification level advocated.

Chapter III. Secrecy Systems

Article 21. The management of state secret carriers should comply with the following provisions:

1. The making of a state secret carrier should be undertaken by an organ or entity or by an entity that has gone through secrecy clearance by the secrecy administrative departments and the production site should comply with secrecy requirements.
2. When receiving or delivering a state secret carrier, the formalities of sorting and counting, indexing, registration and signing for the receipt of the state secret carrier should be observed.
3. Transmission of state secret carriers should be done through channels of confidential transportation, confidential communication or other means that comply with secrecy requirements.
4. The copying of a state secret carrier or extraction, quoting, or compiling contents that are within the scope of state secrets should be reported for approval in accordance with relevant regulations. The classification level, secrecy period or access scope of the original state secret shall not be changed without authorization. The copy of a state secret carrier should be stamped with the seal of the organ or entity that made the copy and be managed the same as the original.
5. The sites, facilities and equipment for keeping state secret carriers should comply with state secrecy requirements.
6. The maintenance and repair of a state secret carrier should be the responsibility of specially designated technicians of the organ or entity that keeps the state secret carrier. If outside personnel are needed for the maintenance or repair, personnel of the organ or entity where the state secret carrier is kept should supervise the whole process on site. If it is truly necessary for a state secret carrier to be repaired outside of the organ or entity, it should be carried out in compliance with state secrecy provisions.

7. Taking out a state secret carrier should comply with state secrecy provisions; and taking a state secret carrier out of the country should be handled in accordance with state secrecy provisions on the formalities for approval and authorization.

Article 22. The destruction of state secret carriers should comply with state secrecy provisions and standards to insure the state secret information can never be restored.

When destroying state secret carriers, the formalities of sorting and counting, registration, reviewing and approval should be observed and they shall be sent to state secret carrier destruction agencies set up by the secrecy administrative departments, or entities designated by secrecy administrative departments. If, as truly required by their work, organs or entities need to destroy a small amount of state secret carriers themselves, they should use equipment and methods that comply with state secrecy standards.

Article 23. Classified information systems shall be classified as top secret, secret and confidential according to the degree of their secrecy. Organs and entities should determine the secrecy classification level of their stored classified information systems at the highest secrecy classification level of secrets the system processes, and adopt appropriate security precaution measures in accordance with the protection requirements of each secrecy classification level.

Article 24. Classified information systems shall be subject to inspection and appraisal by secrecy protection appraisal institutions established or authorized by the national secrecy administrative department and the examination by secrecy administrative departments at the level of municipalities divided into districts and autonomous prefecture before they may be put into use.

The management measures for putting classified information systems of public security and state security organs into use shall be separately stipulated by the national secrecy administrative department together with the public security and state security departments.

Article 25. Organs and entities should strengthen the management of operation and use of classified information systems, appoint specific institutions or personnel to be responsible respectively for the operational maintenance, security and secrecy protection management, and security audits, and regularly conduct security and secrecy protection inspections and risk assessments.

When the secrecy classification levels, the major business applications, scope of use and environment of operation of classified information systems experience changed or the classified information systems are no long in use, this should be reported promptly to the secrecy administrative departments and appropriate measures adopted in accordance with state secrecy provisions.

Article 26. When organs and entities procure projects, goods and services involving state secrets, they should determine the secrecy classification levels in accordance with state secrecy provisions and comply with state secrecy provisions and standards. The organs and entities

should inform the entities providing the projects, goods and services of the requirements for secrecy protection management and sign secrecy protection agreements with them.

Government procurement and supervision administrative departments and secrecy administrative departments should strengthen supervision and management in accordance with the law of the procurement of projects, goods and services involving state secrets.

Article 27. The sponsor of a meeting or other activity that involves state secrets should take the following secrecy protection measures:

1. Determine the secrecy classification level for the meeting or activity on the basis of its contents, formulate a secrecy protection plan, and limit the scope of its participants;
2. Use only sites and equipment that comply with state secrecy provisions and standards;
3. Manage carriers of state secrets in accordance with state secrecy provisions; and
4. Specify secrecy requirements relating to the participants.

Article 28. Enterprises or public institutions engaging in the production, reproduction, maintenance and repair, or destruction of state secret carriers, the integration of classified information systems, scientific research or manufacturing of weaponry, or other business involving state secrets (hereafter referred to as "**classified business**") should be subject to secrecy examination by the secrecy administrative departments together with relevant departments. They may not engage in classified business without clearing secrecy examination.

Article 29. Enterprises and public institutions engaging in classified business should meet the following basic conditions:

1. They shall be legal persons established in accordance with law for three years or more within the territory of the People's Republic of China, and without any criminal record;
2. Their personnel engaged in classified business shall be Chinese citizens within the territory of the People's Republic of China;
3. They shall have sound secrecy protection systems and specialized offices or personnel responsible for secrecy work;
4. The sites, facilities and equipment used in the classified business shall comply with state secrecy provisions and standards;
5. They shall possess the professional competence to undertake classified business; and
6. Other conditions stipulated by law, administrative regulation or the national secrecy administrative department.

Article 30. Specific measures on such matters as the categories and management of classified personnel, the appointment or employment examination, management of separation periods, and rights and interests protection shall be formulated by the national secrecy administrative department together with relevant departments of the State Council.

Chapter IV. Supervision and Management

Article 31. Organs and entities should submit annual reports on the situation of their secrecy work to the secrecy administrative departments of at the same level. Secrecy administrative departments at lower levels should submit annual reports on the situation of the secrecy work in their respective administrative areas to the secrecy administrative departments at the higher level.

Article 32. The secrecy administrative departments shall conduct, in accordance with the law, inspections on enforcement of secrecy laws and regulations by organs and entities in the following areas:

1. Implementation of the secrecy work responsibility system;
2. Development of secrecy systems;
3. Publicity, education and training on secrecy;
4. The management of classified personnel;
5. The determination, modification and declassification of state secrets;
6. The management of state secrets carriers;
7. The secrecy management of information systems and information equipment;
8. The secrecy management of Internet use;
9. The deployment and use of facilities and equipment for protecting secrecy technologies;
10. The management of classified sites and strategic secrecy departments and posts;
11. The management of classified meetings and activities; and
12. Secrecy examination for disclosing government information.

Article 33. If in the course of conducting a secrecy inspection, a secrecy administrative department discovers a leakage vulnerability, it may search relevant materials, question personnel, and make records of the situation; relevant facilities, equipment and documents and materials may in accordance with law be registered for anticipatory preservation and when necessary secrecy technology detection shall be carried out. The organs and entities and their work personal should cooperate with the secrecy examination.

After conducting an inspection, the secrecy administrative department should issue an inspection opinion and, if reform or improvement is required, it should make clear the content of and deadline for the reform or improvement.

Article 34. When an organ or entity discovers that a state secret has been leaked or might be leaked, it should immediately take remedial measures and report the matter within 24 hours to the secrecy administrative department at the same level of government and the department in charge at the higher level.

After the local secrecy administrative departments at various levels receive a report of a leak, they should report the matter within 24 hours level by level up to the national secrecy administrative department.

Article 35. When secrecy administrative departments receive leads or cases of suspected state secrets leaks from citizen complaints, reports by organs or entities, discoveries during a secrecy examination or transfers from relevant departments they should in accordance with law immediately investigate or organize and urge the relevant organ or entity to investigate and handle the matter. After the investigative work has been concluded, if there are facts indicating laws or regulations on protecting state secrets have been violated and that liability needs to be pursued, the secrecy administrative department concerned may make suggestions to the relevant organ or entity on how to handle the matter. The relevant organ or entity should promptly notify in writing the secrecy administrative department at the same level on the results.

Article 36. Illegally acquired or possessed state secrets carriers seized by a secrecy administrative department should be registered and a list of the seized carriers should be made, clearly identifying the secrecy classification level, quantity, source and scope of exposure of, and appropriate secrecy measures shall be adopted.

The secrecy administrative departments may request such relevant departments as the public security and industry and commerce administrative departments to assist in seizing illegally acquired or possessed state secrets carriers, and the relevant department should cooperate.

Article 37. The national secrecy administrative department or the secrecy administrative departments of the provinces, autonomous regions and municipalities directly under the Central Government should, on the basis of secrecy laws and regulations and the scope of secrecy items, appraise whether a relevant item submitted by an organ that is handling a case of a suspected state secrets leak is a state secret and, if so, appraise its secrecy classification.

The secrecy administrative departments should conclude the appraisal of the secrecy classification level and issue an appraisal conclusion within 30 days after accepting the appraisal application. If it cannot issue an appraisal conclusion on time, the deadline may be extended by 30 days with the approval of the responsible person of that secrecy administrative department.

Article 38. Secrecy administrative departments and their work personnel should carry our secrecy examinations, secrecy inspections and investigation of cases of state secrets leaks in accordance with their statutory powers and procedures, and in a scientific, fair, strict and highly efficient manner, and may not use their power to seek personal benefit.

Chapter V. Legal Liability

Article 39. Where an organ or entity fails to report and adopt remedial measures in accordance with provisions after it discovers a secrecy leak case, disciplinary action shall be taken against the directly responsible personnel in charge and other directly responsible personnel in accordance with the law.

Article 40. If, in the course of a secrecy inspection or investigation and handling of state secret leak cases, a relevant organ or entity and their work personnel refuse to cooperate, engage in fraud, hide or destroy evidence or uses other means to avoid or obstruct the secrecy inspection

or investigation of a state secret leak case, disciplinary action shall be taken against the directly responsible personnel in charge and other directly responsible personnel in accordance with the law.

If enterprises or public institutions and their work personnel assist organs or entities to avoid or obstruct secrecy inspections or investigation and handling of state secret leak cases, the relevant departments in charge should take disciplinary actions against them in accordance with the law.

Article 41. If an enterprise or public institution that has gone through secrecy clearance violates provisions on secrecy management, the secrecy administrative department shall order it to correct its ways within a certain time limit. If no corrections are made after the time limit or the corrections made do not comply with requirements, its classified business shall be suspended. If the circumstances are serious, is shall cease its classified business.

Article 42. If a classified information system has been put into use without undergoing testing, evaluation and examination, in accordance with provisions, the secrecy administrative department shall order the organ or entity concerned to correct the situation and recommend that the relevant organ or entity take disciplinary action against the personnel in charge who are directly responsible and other directly responsible personnel in accordance with the law.

Article 43. If an organ or entity entrusts entities that have not undergone secrecy clearance to engage in classified business, the organ or entity concerned shall take disciplinary action against the personnel in charge who are directly responsible and other directly responsible personnel in accordance with the law.

If an entity without secrecy clearance engages in classified business, the secrecy administrative department shall order it to stop its actions that violate the law. Any illegal income shall be confiscated by the department of industry and commerce administration.

Article 44. If secrecy administrative departments have not carried out their duties in accordance with the law, or have abused their powers, or [been guilty of] dereliction of duty or practicing favoritism, disciplinary action shall be taken against the personnel in charge who are directly responsible and other directly responsible personnel in accordance with the law. If the action constitutes a crime, criminal liability shall be pursued.

Chapter VI. Supplementary Provisions

Article 45. These Regulations shall be implemented as of March 1, 2014. The Measures for Implementing the Law of the People's Republic of China on Safeguarding State Secrets approved by the State Council on May 25, 1990 and issued on May 25, 1990 shall be abolished at the same time.

Vocabulary from Chinese State Secrets Law

Safeguarding state secrets	保守国家秘密
Secrecy [protection]	保密
National secrecy administrative department	国家保密行政管理部门
Secrecy management duties	保密管理职责
Classification level	密级
Scope of classified matters	保密事项范围 (art 2(5))
Secrecy clearance inspections	保密检查
Equipment research and development and equipment plans	装备研发、配备计划
Leak or divulge	泄露
Leak secrets	泄密
Secrecy leak-related cases	泄密案件
Secrecy examination	保密审查 (art. 2(7); art. 14 OGIR)
Secrecy administrative departments	保密行政管理部门
Programs	规划
Plans	计划
Entity involved with state secrets	涉及国家秘密的单位 (art. 5)
Release or announce	发布
To classify	定密
State secret classifiers	定密责任人
Classified	涉密
State secrets determination, modification and declassification	国家秘密确定、变更和解除
Originate	产生
Scope of responsibility	职责范围
Scope of access; access scope	知悉范围
Secrecy period	保密期限
Classified	涉密
Classification level	密级
classification authority	定密权限
classification delegation	定密授权
Preliminarily propose a classification level	先行拟定密级
Mark, label	标志
Bear; be marked with	标注
State secret carriers	国家秘密载体
Clear and easy to identify	明显并易于识别
Classified information systems	涉密信息系统
Security measures for secrecy protection	安全保密防护措施 (art. 28)
Confidential (communication)	机要
Appraisal institutions	测评机构
National security sector	国家安全部门

Business involving state secrets	涉及国家秘密的业务
Classified business	涉密业务
Secrecy clearance	保密审查合格 [证书] (art.38, Regs)
Classified personnel	涉密人员
Classified qualification clearance	涉密资格审查 (art. 44)
Classification separation management	脱密期管理
Inspection	检查
Examination	审查
Verify	核查
Review	复查
Confiscate	没收
Appraise	鉴定
Assessment	考核