Checklist for Reporting an Economic Espionage or Theft of Trade Secrets Offense

If you or your company have become the victim of a theft of trade secrets or economic espionage offense, fill out the information below and contact a federal law enforcement official to report the offense.

Background and Contact Information

1. Victim's Name
2. Primary Location and Address
3. Nature of Primary Business
4. Law Enforcement Contact

Description of the Trade Secret

5. Generally describe the trade secret (e.g., source code, formula)
6. Provide an estimated value of the trade secret identifying ONE of the methods and indicating ONE of the ranges listed below

Method:

___Cost to Develop the Trade Secret;

___Acquisition Cost (identify date and source of acquisition); or

___Fair Market Value if sold

Estimated Value:

___Under $50,000;

___Between $50,000 and $100,000;

___Between $100,000 and $1 million;

___Between $1 million and $5 million; or

___Over $5 million

Some means to establish the economic value may include:

- competitive advantages for the owner in using the trade secret;
- the costs for an outsider to duplicate the trade secret;
- lost advantages to the trade secret owner resulting from disclosure to competitors; or
- statements by the defendant about the value of the trade secret.

7. Identify a person knowledgeable about valuation, including that person's contact information.
8. Identify why the item or information is valued as a trade secret. What makes it unique?
9. Does the trade secret have dual application (i.e. civilian and military use)? If so, identify how?
10. Is the trade secret export controlled? If so, identify the reason or regulation?
11. To what extent is the trade secret, or parts of it, publically available or ascertained?

General Physical Measures Taken to Protect the Trade Secret

12. Describe the general physical security precautions taken by the company, such as fencing the perimeter of the premises, visitor control systems, using alarming or self-locking doors or hiring security personnel.
13. Has the company established physical barriers to prevent unauthorized viewing or access to the trade secret, such as "Authorized Personnel Only" signs at access points? (For computer-stored trade secrets see below.)
14. Does the company require sign in/out procedures for access to and return of trade secret materials?
15. Are employees required to wear identification badges?
16. How many employees have access to the trade secret?
17. Was access to the trade secret limited to a "need to know" basis?

18. Does the company have a written security policy?

    (a) How are employees advised of the security policy?

    (b) Are employees required to sign a written acknowledgment of the security policy?

    (c) Identify the person most knowledgeable about matters relating to the security policy, including title and contact information.

Confidentiality and Non-Disclosure Agreements

19. Does the company enter into confidentiality and non-disclosure agreements with employees and third-parties concerning the trade secret?

20. Has the company established and distributed written confidentiality policies to all employees?

21. Does the company have a policy for advising company employees regarding the company's trade secrets?

Computer-Stored Trade Secrets

22. If the trade secret is computer source code or other computer-stored information, how is access regulated (e.g., are employees given unique user names and passwords)?

23. If the company stores the trade secret on a computer network, is the network protected by a firewall?

24. Is remote access permitted into the computer network?

25. Is the trade secret maintained on a separate computer server?

26. Does the company prohibit employees from bringing outside computer programs or storage media to the premises?

27. Does the company maintain electronic access records such as computer logs?

Document Control

28. If the trade secret consisted of documents, were they clearly marked "CONFIDENTIAL" or "PROPRIETARY"?

29. Describe the document control procedures employed by the company such as limiting access, sign in/out policies, and utilizing cover sheets.

30. Was there a written policy concerning document control procedures, and if so, how were employees advised of it?

31. Identify the person most knowledgeable about the document control procedures, including title and contact information.

Employee Controls

32. Are new employees subject to a background investigation?

33. Does the company hold "exit interviews" to remind departing employees of their obligation not to disclose trade secrets?

34. Does the company track personal foreign travel of its employees and provide threat briefings/debriefings?

35. Does the company have a reporting policy for foreign contacts of its employees?

Description of the Theft of Trade Secret

36. Identify the name(s) or location(s) of possible suspects, including name, phone number, email address, physical address, employer, and reason for suspicion.

37. Was the trade secret stolen to benefit a third party, such as a competitor or another business? If so, identify that business and its location.

38. Do you have any information that the theft of trade secrets was committed to benefit a foreign government or instrumentality of a foreign government? If so, identify the foreign government and describe that information.

39. If the suspect is a current or former employee, describe all confidentiality and non-disclosure agreements in effect.

40. Identify any physical locations tied to the theft of trade secret, such as where it may be currently stored or used.

41. If you have conducted an internal investigation into the theft or counterfeiting activities, please describe any evidence acquired.

Civil Enforcement Proceedings

42. Has a civil enforcement action been filed against the suspects identified above?

(a) If so, identify the following:

Name of court and case number:

Date of filing:

Names of attorneys:

Status of case:

(b) If not, is a civil action contemplated? What type and when?

43. Please provide any information concerning the suspected crime not described above that you believe might assist law enforcement.

Relevant Federal Statutes

18 U.S.C. § 1831. Economic Espionage

(a) In general.— Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly –

(1) steals, or without authorization copies, duplicates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;
(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;
(3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
(4) attempts to commit any offense described in any of paragraphs (1) through (3); or
(5) conspires with one or more persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,

shall, except as provided in subsection (b), be fined not more than $500,000 or imprisoned not more than 15 years, or both.

(b) Organizations.— Any organization that commits any offense described in subsection (a) shall be fined not more than $10,000,000.

Statute Limitations: 5 years

18 U.S.C. § 1832. Theft of Trade Secrets

(a) Whoever, with the intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will injure any owner of that trade secret, knowingly--

(1) steals, or without authorization copies, duplicates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;
(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;
(3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
(4) attempts to commit any offense described in paragraphs (1) through (3); or
(5) conspires with one or more persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,

shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

(b) Any organization that commits any offense described in subsection (a) shall be fined not more than $5,000,000.

Statute Limitations: 5 years

18 U.S.C. § 1839. Definitions

(1) The term "**foreign instrumentality**" means any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government;
(2) The term "**foreign agent**" means any officer, employee, proxy, servant, delegate, or representative of a foreign government;
(3) The term "**trade secret**" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if -

(A) The owner thereof has taken reasonable measures to keep such information secret; and

(B) The information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public.

(4) The term "**owner**", which respect to a trade secret, means the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed.

NOTE ON CONFIDENTIALITY: Federal law provides that courts "shall enter such orders and take such action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws." 18 U.S.C. § 1835. Prosecutors utilizing any of the information set forth above will generally request the court to enter an order to preserve the status of the information as a trade secret and prevent its unnecessary and harmful disclosure.