DePaul University

From the SelectedWorks of Barry Kellman

Winter 1995

Disarmament and Disclosure: How Arms Control Verification Can Proceed without Threatening Confidential Business Information

Barry Kellman, DePaul University
David S. Gualtieri
Edward A. Tanzman

Available at: https://works.bepress.com/barry-kellman/24/
Disarmament and Disclosure:
How Arms Control Verification Can Proceed Without Threatening
Confidential Business Information

Barry Kellman*
David S. Gualtieri**
Edward A. Tanzman***

Table of Contents

I. Introduction ...................................... 72
II. Arms Control Verification — New Modalities .......... 77
   A. START Verification: Special Access Visits .......... 78
      1. Requesting a Special Access Visit ............... 79
      2. Pre-Inspection Activities ....................... 81
      3. Inspection Activities .......................... 82
         a. Photographs and Interviews .................. 82
         b. Inspections of Vehicles and Perimeter Patrols .. 83
         c. Mass Media Access ........................... 83
      4. Post-Inspection Activities ...................... 83
      5. CBI Protection Provisions ....................... 84
   B. The Chemical Weapons Convention ................ 84
      1. Declaration Requirements ....................... 86
      2. Inspections .................................. 87
         a. Routine Inspections ......................... 88
            i. Document Searches and Photography .......... 91
            ii. Interviews of Personnel ................... 92
            iii. Post-Inspection Activities ............... 92
         b. Challenge Inspections ....................... 92
            i. Pre-inspection Activities ................ 94

* Professor, DePaul University College of Law.
** Assistant Energy and Environmental Programs Attorney, Argonne National Laboratory.
*** Manager, Economics and Law Section, Decision and Information Sciences Division, Argonne National Laboratory. Work supported in part by BDM International, Inc. under a subcontract with Argonne National Laboratory, which is operated by the U.S. Department of Energy (W-31-109-ENG-38). The opinions expressed herein are those of the authors and not necessarily those of Argonne National Laboratory or its sponsors.
I. INTRODUCTION

International security requires reductions in the quantity and availability of catastrophic weaponry.\(^1\) Arms control negotiators are responding...
to this challenge by finalizing pivotal new initiatives. This progress should, however, be met with more than mere applause—the implications of arms control must be understood, potential problems must be identified, and solutions must be proposed.

In this Article, we examine an issue raised by the Strategic Arms Reduction Treaty (START)\(^3\) and the Chemical Weapons Convention (CWC):\(^4\) how to verify compliance while protecting confidential business information (CBI).\(^5\) The concern is that the verification of arms control treaties requires the ability to investigate private industrial activities, and that this requirement risks revelation of valuable information in an uncertain legal environment.\(^6\) Since cooperation from the cal weapons, biological weapons, and ballistic missiles. These weapons would, if used, necessarily devastate civilian populations. See generally Barry Kellman, Bridling the International Trade of Catastrophic Weaponry, 43 AM. U. L. REV. 755 (1994) (discussing catastrophic weaponry and suggesting measures to limit their trade).


5. The term “confidential business information” (CBI) refers to business-related information that gives its holder a commercial advantage because it is not widely known to competitors or the general public. CBI can consist of technical or non-technical forms of information, including: formulas, patterns, compilations, programs, devices, methods, techniques, drawings, processes, financial data, price codes, customer lists, economic studies, cost reports, and bookkeeping methods. This term is widely used in arms control policy discussions. See, e.g., CONGRESS OF THE UNITED STATES OFFICE OF TECHNOLOGY ASSESSMENT, The Chemical Weapons Convention: Effect on the United States Chemical Industry (1993) [hereinafter OTA REPORT].

Some courts have distinguished between trade secrets and other confidential business and financial information but have not set forward criteria as to the content of that distinction. While "confidential business information has long been recognized as property," Carpenter v. United States, 484 U.S. 19, 26 (1987), the mere fact that business information is confidential and that its disclosure might harm a company’s commercial position does not automatically entitle it to the same protections as trade secrets. See Littlejohn v. BIC Corp., 851 F.2d 673, 685 (3d Cir. 1988) ("[N]on-trade secret but confidential business information is not entitled to the same level of protection from disclosure as trade secret information."). The authors do not discern any meaningful difference between the content of “CBI” and of “trade secrets” that could be relevant to the problem of protecting business information from arms control-related revelation. As this Article’s primary focus is arms control, and because the legal difference between the terms is negligible, “CBI” is used herein.

6. The United States law of trade secret protection derives from two principal sources: (1) UNIFORM TRADE SECRETS ACT, 14 U.L.A. 437 (1990) [hereinafter UTSA], and (2) RESTATEMENT
private sector is essential to the implementation of these treaties, methods must be devised to assure industries of the sanctity of their commercial information.\(^7\)

The threat to CBI stems from the need to gather reliable and objective intelligence in order to monitor the weapons production and acquisition of other nations, either through data reporting requirements or through on-site monitoring and inspections.\(^8\) While past arms control efforts focused on deployed weaponry at government installations and military sites, more recent agreements focus on dual-use technology and substances that are widely possessed by private entities. Consequently, arms control verification entails obtaining data from private industries.\(^9\)

Protection of CBI is critical to the industries that are most likely to be subject to arms control verification. The same technologies that are used in sophisticated weaponry also have important commercial applications; the control of these dual-use technologies demands regulation of highly competitive, leading-edge industries that have invested massively in research and development. In order to recoup their investment and make a profit, it is essential that these firms retain some measure of confidentiality with respect to their technical knowledge. The revelation of CBI can enable a competitor to obtain, at minimal cost, information that its originator acquired through an enormous investment of time and money, thereby erasing the com-

---

7. See John D. Morrocco, Verification Raises Cost, Technology Concerns, AVIATION WK. & SPACE TECH., Aug. 6, 1990, at 44.

8. David Hafemeister et al., The Verification of Compliance with Arms Control Agreements, SCL AM., Mar. 1985, at 38, 39.

petitive advantage created by that initial investment in research and development.  

Additionally, the chemical and nuclear technologies industries participate in an intensely competitive marketplace in which proprietary knowledge is vital to a firm’s success. A company’s competitive edge is often based on techniques that provide small but significant margins of efficiency, yield, and cost, or that result in a product that is more pure, more attractive, or more durable. Moreover, the entire livelihood of firms that concentrate on a niche market or technology may depend on the possession of a few highly specialized trade secrets.

The problem is doubly complicated by the introduction of international inspectors, whose access to private data and equipment heightens the threat of losing CBI to foreign competitors. Currently, United States companies with expertise in dual-use technologies lead the world in many innovative processes. By contrast, their competitors in many other countries use older generations of processes that are more widely known. Consequently, United States firms are likely to be the targets of industrial espionage by foreigners who have little to lose from intrusive verification techniques carried out on their own soil.

Furthermore, the protection of intellectual property varies among nations. Even though several international treaties, organizations, and conventions allow foreigners to obtain intellectual property protection in another state, they do not recognize or protect CBI.

10. See OTA REPORT, supra note 5, at 43-45.
11. Id.
12. Many nations have effective mechanisms of protecting all forms of intellectual property. However, in countries that apply the system of “national treatment,” foreign owners of intellectual property receive whatever protections are afforded to nationals of the state in question. National treatment, though nondiscriminatory, is of little assistance when an intellectual property right is violated in a state with minimal or no protections in place. See Frank J. Garcia, Protection of Intellectual Property Rights in the North American Free Trade Agreement: A Successful Case of Regional Trade Regulation, 8 Am. U. J. Int’l L. & Pol’y 817, 820-32 (1993) (explaining that intellectual property protections are usually limited to those provided by the host country, though noting that possible international agreements might expand this protection in the future). See also BARRY KELLMAN ET AL., DEFENSE NUCLEAR AGENCY TECHNICAL REPORT NO. 93-59, A COMPARATIVE STUDY OF THE CHEMICAL WEAPONS CONVENTION IN FOREIGN JURISDICTIONS (1993) (noting and criticizing practice).
Because CBI has great value, the possibility of its loss threatens companies that might otherwise support arms control. While many firms might tolerate the inconvenience of reporting requirements and inspections as a cost of attaining a more peaceful world, endangering CBI in a way that could literally put the firms out of business is likely to incur opposition. Since the cooperation of these firms is essential to the success of recent arms control regimes, widespread concern over the loss of CBI could potentially impede their implementation. Thus, CBI protection is necessary both as a matter of fairness to commercial firms that have property interests that deserve protection, and as a matter of arms control policy.

CBI could be lost as a result of arms control activities through two distinguishable but comparably damaging scenarios. First, arms control inspectors or regulatory officials (either foreign or of the United States) could wrongfully divulge CBI that they acquire during inspections or deduce from treaty-required declarations. Second, agencies of the United States government could divulge, through operation of law, CBI that is rightfully in their possession due to arms control requirements.

Without adequate CBI protection, a perilous situation could develop where a private company would have to choose between obstructing arms control verification and losing valuable business information. It is even possible that the company could be tempted to seek judicial injunctive relief from a forthcoming inspection or reporting requirement by claiming that its constitutional property rights could be violated by arms control operations. If a United States court were to enjoin arms control verification activities, however, the United States might be perceived as having violated its obligation to comply with the treaty.

Recent developments springing from side agreements concluded during the Uruguay round negotiations of the General Agreement on Tariffs and Trade (GATT) suggest improvements in the international regime to protect intellectual property. The Agreement on Trade Related Aspects of Intellectual Property Rights, Including Trade in Counterfeit Goods (TRIPs) establishes new standards for the protection of many forms of intellectual property, including trade secrets, and requires mechanisms for the enforcement of rights both internally and at the borders. See Michael L. Doane, TRIPs and International Intellectual Property Protection in an Age of Advancing Technology, 9 AM. U. INT'L L. & POL'Y 465, 468 (1994). However, it is not expected that TRIPs will result in significant changes in trade secret protection under U.S. federal law. Daily Rep. for Executives (BNA), Summary of HR 5110, “Uruguay Round Agreements Act” Prepared by Clinton Administration, Sept. 27, 1994.

14. See, e.g., David A. Koplow & Philip G. Schrag, Carrying a Big Carrot: Linking Multilateral Disarmament and Development Assistance, 91 COLUM. L. REV. 993, 1021 n.116 (1991) (“The fear of exposing valuable trade secrets has been the single biggest concern that the American chemical industry has expressed about the new chemical weapons convention . . . .”).

Therefore, it should be the policy of the United States to implement carefully designed CBI protection measures. Fortunately, many of the proposed initiatives can be modeled on federal statutes with similar measures. The government must work closely with private companies, urging them to employ initiatives designed to minimize the amount of CBI disclosed and to protect any CBI that must be revealed.

The Article consists of three additional parts. Part II describes in detail the modalities of arms control verification, focusing on two recently signed agreements: the Strategic Arms Reduction Treaty and the Chemical Weapons Convention. Parts III and IV address the threat that verifying these treaties poses to the confidentiality of valuable information. Part III considers problems of CBI loss due to the activities of inspectors and officials gaining access to private information. Part IV considers the possibility that CBI will be lost due to the operation of United States law. Each part suggests strategies to protect CBI and provides examples of relevant federal legislation.

II. ARMS CONTROL VERIFICATION—NEW MODALITIES

Historically, arms control treaties have sought to limit the number of deployed weapons systems. With few exceptions, those treaties have had little direct impact on private industry.16 The impact of arms control on private industry changed radically during the 1980s when at least two strategic justifications converged to magnify the importance of intrusive verification to arms control.

First, President Reagan’s admonition of the need to “[t]rust, but verify” made direct verification of the terms and conditions of arms control treaties central to their negotiation and conclusion.17 Since arms control treaties put a ceiling on arms escalation, verification helped alleviate the fear that an undetected breach by one party could enable it to “break out” in a sudden and devastatingly successful attack.18 More trenchant was the emerging view that vigorous verification would enable one party to assert that another party was in non-
compliance and to present evidence of a breach to the world community, whose diminished opinion of the accused would be the only real means of accountability.  

Second, during the 1980s, arms control increasingly focused on the problem of weapons proliferation. Critical to controlling proliferation is controlling the means of weapons production rather than merely limiting their deployment. In this view, the possession of catastrophic weapons, and not the inclination of a government to use them, is the offensive activity. Furthermore, advances in technology that tend to make weapons more concealable demand that verification of weapons non-production be increasingly more intrusive in order to be effective.

Two new arms control agreements illustrate the incorporation of intrusive verification mechanisms. START is a preeminent example of a bilateral superpower nuclear arms limitation agreement. The CWC is, by contrast, a global effort to eliminate an entire category of weapons. Its comprehensive nature and rigorous standards offer a compelling illustration of a new mode of arms control. In this part, we will discuss the modes of verification employed by these treaties to demonstrate the risks posed to CBI.

A. START Verification: Special Access Visits

START is an extremely detailed and voluminous international agreement that represents a watershed in the history of arms control. The bulk of the treaty concerns specific requirements for the reduction and


19. See Patricia B. McFate, Where Do We Go From Here? Verifying Future Arms-Control Agreements, WASH. Q., Autumn 1992, at 75, 77 ("The criterion of political significance—the view that every deviation from the provisions of an agreement is a violation of an international relationship—leads to insistence on intrusive, extensive verification . . . "). See also David Aaron, Verification: Will It Work?, N.Y. TIMES, Oct. 11, 1987, at 37; Trimble, supra note 2, at 890–93.


24. START, supra note 3.

25. CWC, supra note 4. Two important parts of the CWC in relation to CBI are the Annex on Implementation and Verification [hereinafter Verification Annex] and the Annex on the Protection of Confidential Information [hereinafter Confidentiality Annex].
limitation of nuclear arsenals. The Parties to START\(^{26}\) have explicitly recognized that the reduction and limitation of strategic offensive arms “will help to reduce the risk of outbreak of nuclear war and strengthen international peace and security.”\(^{27}\) According to article I, each Party agrees to reduce and limit its strategic offensive arms in accord with the terms of the treaty. In addition, each Party is required to comply with all other obligations set forth in the treaty, its annexes, protocols and memoranda of understanding.\(^{28}\)

To verify compliance with START provisions, each Party has the right to conduct inspections and continuous monitoring activities at declared facilities under the provisions of the Inspection Protocol.\(^{29}\) START provides for thirteen types of inspections of declared facilities with varying aims, and different provisions of the Inspection Protocol govern each type of inspection.\(^{30}\) These inspections, except for Special Access Visits (SAVs), will take place almost exclusively at government-owned facilities and therefore will not threaten CBI at privately owned facilities.

1. Requesting a Special Access Visit

START established the Joint Compliance and Inspection Commission (JCIC) to promote the objectives and implementation of the treaty.\(^{31}\) At the request of any Party, the JCIC will be convened to: (1) resolve questions about compliance; (2) agree upon additional measures necessary to improve START’s viability and effectiveness; and (3) resolve questions about the applicability of the treaty to new kinds of strategic offensive arms.\(^{32}\) The requested Party has fourteen days to respond to

---

26. START was negotiated and signed as a bilateral agreement, but due to unforeseen events in the former Soviet Union, the START agreement is now multilateral. On May 23, 1992, all of the former Soviet republics that then had strategic nuclear weapons (Belarus, Kazakhstan, Russia, and Ukraine) signed the Lisbon Protocol and became Parties to START. See Protocol to the Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Reduction and Limitation of Strategic Offensive Arms, May 23, 1992, S. TREATY Doc. No. 32, 102d Cong., 2d Sess. (1992). See also U.S., Four Commonwealth States Sign START Protocol in Lisbon, ARMS CONTROL TODAY, June 1992, at 18. Since then, Belarus, Kazakhstan, and Ukraine have agreed to allow Russia to dismantle their weapons in exchange for United States economic assistance. Douglas Jehl, Ukrainian Agrees to Dismantle A-Arms, N.Y. TIMES, Jan. 13, 1994, at A6.

27. START, supra note 3, Preamble.

28. Id. art. I.

29. Id. art. XI, para. 1. For a list of the facilities declared by each Party under the treaty, see id. Two protocols to START govern the conduct of special access visits: the Protocol on Inspections and Continuous Monitoring Activities, S. TREATY Doc. No. 20, at 102 [hereinafter Inspection Protocol] and the Protocol on the Joint Compliance and Inspection Commission Relating to Treaty, S. TREATY Doc. No. 20, at 319 [hereinafter JCIC Protocol].

30. See id. art. XI, paras. 2–13.

31. Id. art. XV.

32. Id. art. XV, para. 13 (a)–(c). The work of the JCIC will be confidential. The JCIC may
a request that the JCIC be convened. A session of the JCIC then must be convened as soon as possible.

A Party may also request that the JCIC be convened in a "Special Session" to address urgent concerns relating to the compliance of a Party. The request may contain a proposal for resolving the concern that may include, but is not limited to, a "visit with special right of access," or SAV, to the facility or location where the activity causing the concern took place in order to address questions of noncompliance. Since SAVs are not mandatory, the challenged Party may refuse the request.

The requested Party has seven days to accept the proposed date and location for the Special Session or propose an alternate date and location. A response may also include an acceptance of the proposed method for resolving the concern including the date, location, and procedures for a proposed SAV, or a proposal for a specific method for resolving the concern, including the date, location, and procedures for a SAV. If the Parties agree to a SAV or another method of resolving the concern, they can agree not to convene the Special Session. While application of the Inspection Protocol to SAVs is optional, it is reasonable to believe that the general procedures for inspections already agreed to by the Parties in the Inspection Protocol will be applied to SAVs.

record agreements or the results of its work in an appropriate document. Any agreement so recorded will not be confidential, except as otherwise agreed by the JCIC. JCIC Protocol, supra note 29, art. V.

33. JCIC Protocol, supra note 29, art. II, para. 1. Requests and responses must include the questions the Party intends to raise, the name of the Party's head representative to the JCIC, and the proposed date and location for convening the session. Id. art. II, para. 1(a)–(c).

34. Id. art. II, paras. 2–3.

35. Id. art. III, para. 1. Any request for a special session must include, at a minimum: the nature of the concern (including the kind and type of strategic offensive arms related to the concern); the name of the Party's head representative; and the proposed date and location of the special session. Id. art. III, para. 1(a)–(c).

36. Id. art. III, para. 1. START does not delimit the facilities that could be the subject of a visit with special rights of access (SAV); therefore, SAVs could conceivably be conducted anywhere.

37. "It is the duty of the challenged Party to convince the challenger that the suspicions are unfounded. If this cannot be done, the challenging Party can request a special access visit to the suspicious site, but the challenged Party can refuse such a request." 138 CONG. REC. S15,498 (daily ed. Sept. 29, 1992) (statement of Sen. Pell) (emphasis added).

38. JCIC Protocol, supra note 29, art. III, para. 2(a)–(b).

39. Id. art. III, para. 3(a)–(b).

40. Id. art. III, para. 3.

41. "Visits with special right of access may be conducted in accordance with the provisions of the Inspection Protocol, as applicable." Id. art. III, para. 3 (emphasis added).
2. Pre-Inspection Activities

Each Party must provide notice of inspections and continuous monitoring activities.\(^{42}\) No specific notification requirements apply to SAVs apart from the request and response requirements for convening a Special Session of the JCIC.\(^{43}\) For inspections of declared facilities, notification periods range from sixteen to seventy-two hours; generally, the inspecting Party must supply the following information: the point of entry to the inspected site, the date and time of arrival, the inspection site, the type of inspection, and the names of inspectors and aircrew members.\(^{44}\)

To expedite entry, an in-state escort, including representatives of the inspected facility, will meet the inspection team and monitors upon arrival at the point of entry.\(^{45}\) The in-state escort has the obligation and right to accompany the inspection team and assist them in exercising their functions throughout the in-state period.\(^{46}\)

Inspectors and monitors will enjoy special privileges and immunities during their entire stay within the territory of the inspected Party.\(^{47}\) The number of permissible inspectors ranges from ten to twenty, depending on the type of inspection. The number of monitors ranges from five to thirty, depending on the function being performed. No more than one inspection or monitoring team will be permitted at an inspection site, though the inspection team can be divided into subgroups.\(^{48}\)

Pre-inspection procedures and any necessary briefings will begin upon the arrival of inspectors and monitors at the inspection site and must be completed within one hour.\(^{49}\) Prior to completing pre-inspection procedures, the inspection team leader will be permitted to designate a subgroup of inspectors to inspect vehicles leaving the inspect-
The inspection of vehicles cannot hamper the operation of the facility.  

3. Inspection Activities

Inspectors and monitors must not interfere with, delay, or hamper ongoing activities at the inspection site or facility subject to monitoring. In addition, no actions of the inspectors or monitors can affect the safe operation of a facility. The duration of an inspection depends on the type of inspection taking place. Extensions of no more than eight hours can be negotiated by the Parties in order to complete inspections.

If, during the course of an inspection, inspectors, monitors, or the in-state escort contravene the rules and procedures governing inspections, the in-state escort can inform the leader of the inspection or monitoring team. The respective team leader will then be required to take measures to prevent the recurrence of such actions. If these measures fail to resolve the issue, the in-state escort may include a statement in the inspection or continuous monitoring report to which the team leader will be allowed to respond.

a. Photographs and Interviews

Only representatives of the inspected Party may photograph or operate a camera during inspection or monitoring activities. If inspectors or monitors so request, an in-state escort will take two photographs of each object or building within the inspection site or the perimeter continuous monitoring area. Inspectors or monitors will designate these sites as relating to the suspected noncompliance or ambiguity. Inspectors and monitors are to communicate with personnel of the inspected Party only through the in-state escort.

50. Id. art. VI, para. 30. If such a subgroup is not designated, vehicles will remain free to depart the facility.

51. Id. art. VI, para. 6. In carrying out their activities, inspectors and monitors must observe safety regulations established at the inspection site. They must also follow regulations for protecting equipment and maintaining a controlled environment within a facility. To implement safety procedures, the in-state escort must provide a safety briefing and any necessary protective gear. Id. art. VI, para. 7.

52. Id. art. VI, para. 31.

53. Id. art. VI, para. 9.

54. Id. art. VI, para. 18.

55. Id. Each Party retains one photograph of each item. The photographic equipment provided by the inspected Party must be capable of producing instant development photographs.

56. Id. art. VI, para. 5.
b. Inspections of Vehicles and Perimeter Patrols

Before inspecting a particular structure within an inspection site, inspectors may station themselves at the exits to the structure and inspect any object, container, or vehicle leaving the structure.\textsuperscript{57} Inspectors also have the right to patrol the perimeter of an inspection site and to be present at the exits of the inspection site. Vehicles will not be permitted to leave the inspection site until they have been inspected or until the inspection team indicates that it does not wish to inspect a particular vehicle.\textsuperscript{58}

c. Mass Media Access

Special procedures govern media coverage of START inspections. At the point of entry, the inspected Party must allow members of the mass media to photograph the arrival and departure of the inspection and monitoring teams.\textsuperscript{59} Interviews of inspectors and monitors may be granted on a case-by-case basis if agreed to by the Parties.\textsuperscript{60} The activities of the mass media cannot interfere with the conduct of inspections or continuous monitoring activities, and the Parties cannot allow members of the mass media to accompany inspectors and monitors during inspections and continuous monitoring activities.\textsuperscript{61}

4. Post-Inspection Activities

The inspection team leader must give the in-state escort an official written inspection report within two hours of the initiation of the post-inspection process.\textsuperscript{62} The inspected Party is entitled to include written comments in the report\textsuperscript{63} and the Parties must, when possible, clarify ambiguities regarding factual information contained in the inspection report. Any relevant clarifications must be recorded in the report.\textsuperscript{64} Post-inspection procedures will begin once the period of inspection ends and must be completed within four hours.\textsuperscript{65}

\textsuperscript{57} Id. art. VI, para. 34.  
\textsuperscript{58} Id. art. VI, para. 35.  
\textsuperscript{59} Id. art. V, para. 22(a).  
\textsuperscript{60} Id. art. V, para. 22(b). Interviews may include the taking of photographs and audio/visual recordings.  
\textsuperscript{61} Id. art. V, para. 22(c)–(d).  
\textsuperscript{62} Id. art. XVIII, para. 1. Reports must contain the following: the type of inspection conducted; the inspection site; the type and number of missiles, stages, launchers, heavy bombers, ballistic missile submarines, and support equipment observed during the inspection. Photographs taken during the inspection as well as diagrams and maps of the inspection site will be considered part of the report.  
\textsuperscript{63} Id. art. XVIII, para. 3.  
\textsuperscript{64} Id. art. XVIII, para. 4.  
\textsuperscript{65} Id. art. VI, para. 32.
5. CBI Protection Provisions

While no provisions of START explicitly refer to trade secrets or CBI, an important inspection procedure prohibits inspectors and monitors from disclosing information obtained during inspection or monitoring activities without the express consent of the inspected Party. This obligation continues even after their assignments as inspectors and monitors end.66

The Parties also addressed under what circumstances START-related information should be released to the public. Under article VIII, section 6, each Party can release to the public all current data that is included in the Memorandum of Understanding, as well as the appended photographs. Geographic coordinates and site diagrams may not be released unless otherwise agreed. The Parties must hold consultations on releasing to the public data and other information provided to each Party pursuant to START. However, article VIII will not hinder communication to individuals who, due to official responsibilities, require such data or other information. Though CBI is not explicitly mentioned, START seems to leave open the possibility that CBI could be disclosed to the public.67

B. The Chemical Weapons Convention

The CWC is an unprecedented multilateral effort to eradicate an entire category of catastrophic weapons and verify their continued absence.68 As such, it has two goals. First, it mandates the declaration and destruction of existing chemical weapon stockpiles and production facilities.69 Destruction of chemical weapons must begin within two years and be completed not later than ten years after the CWC takes effect.70 The destruction of chemical weapons production facilities must begin within one year and be completed not later than ten years after the CWC takes effect.71 Subject to environmental, health, and safety

66. Id. art. VI, para. 2.
68. For a full discussion of the obligations imposed by the CWC, what measures States Parties should take to fulfill those obligations, and the legal implications of those measures, see generally BARRY KELLMAN ET AL., MANUAL FOR NATIONAL IMPLEMENTATION OF THE CHEMICAL WEAPONS CONVENTION (1993).
69. CWC, supra note 4, art. I, (2)-(4).
70. Id. art. IV, (6).
71. Id. art. V, (8).
restrictions, each State Party may destroy its weapons and facilities by a means it chooses, provided their destruction may be verified.

Second, the CWC seeks to verify that states do not initiate or resume chemical weapons production and storage. Verifying nonproduction of chemical weapons is the core of the CWC. Even States Parties with no chemical weapons to be destroyed must comply with the verification measures. While each State Party has the right to produce and use toxic chemicals for legitimate commercial purposes, such production and use carries the concomitant obligation to ensure that these chemicals not be used for purposes prohibited by the CWC. Verification of activities not prohibited by the CWC entails an elaborate mechanism for monitoring all production and acquisition of various chemicals by States Parties.

To accomplish its goals, the CWC creates the Organization for the Prohibition of Chemical Weapons (OPCW), which will monitor the production capabilities and activities of States Parties to ensure that the objectives of the CWC are, in fact, being met. The OPCW will be a powerful international regime vested with extensive legislative, investigative, and enforcement responsibilities. Taken as a whole, it signifies a systematic introduction of international law enforcement into chemical weapons control.

72. Id. art. IV, (10); art. V, (11).
73. Id. art. IV(A), (13).
74. Id. art. IV(A), (13).
75. Id. art. IV(A), (13).
76. See generally THOMAS BERNAUER, UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH, THE CHEMISTRY OF REGIME FORMATION: EXPLAINING INTERNATIONAL COOPERATION FOR A COMPREHENSIVE BAN ON CHEMICAL WEAPONS (1993) (analyzing the driving forces behind international cooperation on chemical weapons controls).
77. Id. art. VI, (1).
78. Id. art. VI, (2)-(8).
79. Id. art. VIII.
80. The OPCW will be comprised of three bodies. The Conference of State Parties will be authorized to enact rules of procedure, assess compliance and resolve issues as to the scope of the CWC. The Executive Council will oversee day-to-day activities, including supervising verification. The Technical Secretariat will have primary responsibility for monitoring and inspecting facilities that could become involved in illegal chemical weapons production. Id. art. VIII.
81. For a discussion of the structure of the OPCW and its principal functions, see A. Walter Dorn & Ann Rolya, The Organization for the Prohibition of Chemical Weapons and the IAEA: A
1. Declaration Requirements

To verify that new chemical weapons are not being produced, the CWC categorizes a wide range of industrial chemicals into three schedules based on both their suitability for use in weaponry and their legitimate commercial value. Schedule 1 contains a list of thirteen "super-toxic lethal chemicals" that (1) are actual warfare agents; (2) pose a particular risk of potential use as chemical weapons; (3) are key precursors with chemical structures closely related to chemical weapons; or (4) pose a high risk of conversion into chemical weapons. Schedule 2 lists chemicals that are key precursor chemicals to warfare agents or are super toxic lethal chemicals not listed in Schedule 1 but pose a significant risk to the objectives of the Convention. Schedule 3 lists chemicals that are also precursors to warfare agents but are both further removed from warfare agents and have other legitimate industrial uses.

States Parties must make initial and annual declarations of the total amount of each scheduled chemical produced, consumed, imported, or exported and the purposes for which these chemicals are obtained or processed, as well as extensive information about production facilities. Declaration requirements vary according to which scheduled chemicals are at the facility. More detailed information must be provided about Schedule 1 chemicals and related facilities than about Schedule 2 chemicals, and likewise, Schedule 3 chemicals require less information than Schedule 2 chemicals.

For example, declarations regarding Schedule 1 chemicals and related facilities include considerable detailed information about the chemicals and related facilities, while declarations regarding Schedules 2 and 3 require less detailed information.
ule 2 and Schedule 3 chemicals and related facilities focus on aggregate national data, on plant sites, and on past production of these chemicals that were used for chemical weapons purposes. Similarly, declarations of Schedule 2 chemicals and related facilities must include the quantities of Schedule 2 chemicals produced or consumed at each plant site, whereas Schedule 3 declarations only require listing the plant sites where these chemicals are produced. In addition, declarations must be made regarding facilities that manufacture organic chemicals beyond certain threshold limits. These facilities are known as “other” or “PSF” chemical production facilities.

2. Inspections

To verify that declarations are correct and to ensure that States Parties are meeting their obligations, the CWC provides for both routine inspections and challenge inspections. Both types of inspections share the common goal of verifying the nonproduction of chemical weapons without interfering with the legal rights of States Parties or their citizens. The CWC’s guiding principle is that on-site inspections be implemented in a manner that avoids undue intrusion into activities engaged in for peaceful purposes.

Whether undue intrusion can be avoided remains a matter of considerable controversy. Certainly, these verification mechanisms will have profound effects on private industry, raising difficult legal questions.

---

90. Initial declarations to be submitted within 30 days after the CWC enters into force for that State Party and annual declarations to be submitted within 90 days after the end of the previous calendar year must include aggregate national data for the previous calendar year. Furthermore, initial and annual declarations are required for all plant sites that comprise one or more plants that produced, processed, or consumed more than the threshold amounts of Schedule 2 chemicals during any of the previous three years or are anticipated to do so in the next calendar year. Finally, within 30 days after the CWC enters into force for each State Party, declarations must be submitted for all plant sites comprising plants that produced at any time since January 1, 1946 a Schedule 2 chemical for chemical weapons purposes any time since January 1, 1946. See id. pt. VII, (1)-(9).

91. The requirements as to aggregate national data and the deadlines for Schedule 3 chemicals are identical to those for Schedule 2 declarations. See id. pt. VIII, (1)-(2).

92. Within 30 days after the CWC enters into force for it, each State Party must submit its list of other chemical production facilities, including information on each plant site. No later than 90 days after the beginning of each following calendar year, annual declarations must provide the information necessary to update the list, including information on the approximate aggregate amount of production of the unscheduled discrete organic chemicals in the previous calendar year. See infra parts II.B.2.a.-b.

93. See infra parts II.B.2.a.-b.

94. CWC, supra note 4, art. VI, (10).

95. CWC verification mechanisms could affect the constitutional rights of private corporations.
Chemical companies will be subjected to additional reporting requirements as a result of the CWC's declarations scheme. Furthermore, preparing for inspections can be expensive. Because of its rigorous requirements and anticipated impact on private industry, the CWC poses new implementation challenges for the United States government.

a. Routine Inspections

Routine inspections are to be carried out at "declared facilities" to permit the Technical Secretariat to verify that annual declarations for these facilities are accurate. Routine inspections are intended to deter violations "in a manner which avoids hampering the economic or technological development of State Parties," and to compile sufficient and individuals. Most important, the possibility of warrantless inspections conducted by international inspectors could violate the Fourth Amendment's prohibition against unreasonable searches and seizures. See Edward A. Tanzman & Barry Kellman, Defense Nuclear Agency Technical Report No. 91-216, Harmonizing the Chemical Weapons Convention with the United States Constitution (1991) [hereinafter Tanzman, Harmonizing]; Edward A. Tanzman, Constitutionality of Warrantless On-Site Arms Control Inspections in the United States, 13 Yale J. Int'l L. 21 (1988); David A. Koplow, Arms Control Inspection: Constitutional Restrictions on Treaty Verification in the United States, 66 N.Y.U. L. Rev. 355 (1991); David G. Gray, "Then the Dogs Died": The Fourth Amendment and Verification of the Chemical Weapons Convention, 94 Colum. L. Rev. 567 (1994). The requirement that penal sanctions be enacted under the CWC combined with the right of inspectors to interview facility personnel also threatens to violate the Fifth Amendment right to be free from compelled self-incrimination. See Tanzman, Harmonizing, supra, at 61–62. See also Burris M. Carnahan, SAIC Report DE-AC01-88DP50066, Constitutional Implications of Implementing a Chemical Weapons Convention (1990); Kevin C. Kennedy, The Constitution and On-Site Inspection, 14 Brook. J. Int'l L. 2 (1988); Eric Hamburg, Arms Control Verification and the U.S. Constitution (Stanford University Center for International Security and Arms Control Working Paper, 1989).

Additional reporting requirements could prove to be the most costly aspect of CWC implementation. See Dan Charles, Chemical Weapons Ban: Now for the Hard Part, New Scientist, Jan. 23, 1993, at 7. Of course, the burden of the reporting requirements will largely depend on the size of the company affected. For instance, some firms will be required to compile complicated and onerous production reports for the first time as a result of CWC requirements. See OTA Report, supra note 5, at 21–24.

To assess how burdensome reporting requirements might be, the United States government is currently considering how CWC reporting requirements might overlap with existing federal regulations such as FIFRA and TSCA and thereby take advantage of existing mechanisms and regulations. See generally Gordon M. Burck & Geoffrey W. Nagler, Chemical and Biological Arms Control Institute Contract No. AC92MC1004, Study of U.S. Regulatory Requirements Related to the Chemicals Covered by the Chemical Weapons Convention (1989). See also OTA Report, supra note 5, at 21–24.

First, facilities may have to shut down operations to prepare for inspections and during the inspections themselves. In addition, in order to protect CBI firms may find it necessary to install shrouds, boxes, and screens, or to reconfigure plant processes to shield CBI. See OTA Report, supra note 5, at 29.


96. Chemical, supra note 4, art. VI, (10)–(11).
accurate information to permit a high degree of accord among the States Parties as to what specific conduct constitutes a violation.

Inspections are to be performed in accordance with the CWC, the rules established by the Director General of the Technical Secretariat, and individual "facility agreements" to be negotiated between a State Party and the OPCW for routine inspections of declared facilities. The inspection team must observe the inspection mandate issued by the Director General and conduct the inspection in a manner that creates the least possible inconvenience and disturbance for the State Party and the inspected facility. In carrying out inspection activities, the inspection team must observe safety regulations established at the inspection site.

The Technical Secretariat must conduct routine inspections of Schedule 1, 2, or 3 facilities, or "other relevant" facilities, in a manner that does not unduly intrude into a State Party's legitimate chemical activities or hamper economic or technological development. Procedures applicable to routine inspections will vary depending on the type of facility being inspected. Each State Party must negotiate facility agreements with the OPCW, which will govern the conduct of inspections of declared Schedule 1 and 2 facilities; agreements may be negotiated with regard to Schedule 3 and "other relevant" facilities. Pursuant to these agreements, the inspection team must be permitted access to search facilities. The model agreements, to be prepared by the Preparatory Commission of the OPCW, will likely outline inspection procedures that may include identification of any future technological changes.

Inspections of Schedule 1 facilities will verify that the quantities of Schedule 1 chemicals are correctly declared. The number, intensity, duration, timing, and mode of inspection of a Schedule 1 facility will

101. Id. pt. II, (39)-(40). The inspection must also be carried out in a manner that does not unnecessarily hamper or delay the operation of a facility or affect its safety. Id. pt. II, (40).
102. Id. pt. II, (43).
103. CWC, supra note 4, art. VI, (10)-(11).
104. Verification Annex, supra note 25, pt. VI, (25)-(27); pt. VII, (24). Facility agreements must be based on a model agreement prepared by the Preparatory Commission of the OPCW. For Schedule 1 facilities, agreements must be concluded within 180 days of the CWC entering into force; for Schedule 2 facilities, 90 days after the initial inspection. Facility agreements are not required for Schedule 3 or other relevant facilities unless requested by the inspected State Party. Id. pt. VIII, (19); pt. IX, (16).
105. Id. pt. II, (45).
106. Id. pt. III, (8). Model facility agreements will be submitted to the Conference of the State Parties for consideration and approval. CWC, supra note 4, art. VIII, (21) (i).
be based on the risk that facility poses to the objectives of the CWC and the characteristics of that facility.\(^{108}\)

Schedule 2 facilities will be inspected to determine that their activities are in accordance with CWC obligations, that their declarations are accurate, and that no Schedule 1 chemicals are at the site.\(^{109}\) Schedule 2 facilities must receive an initial inspection, preferably within three years after the CWC enters into force. This initial inspection is important in determining the frequency and intensity of subsequent inspections. During the initial inspection, the inspectors must assess the characteristics of the facility, the nature of the activities carried out there, and the risk the facility poses to the CWC's objectives.\(^{110}\)

Subsequently, Schedule 2 facilities must be inspected within one year after production, processing, or consumption is first declared.\(^{111}\) In selecting sites for inspection, the Technical Secretariat will consider the above factors and the results of the initial inspection.\(^{112}\) The method used by the Technical Secretariat to choose the facilities to be inspected cannot be predictable.\(^{113}\) Apart from challenge inspections, no facility can be inspected more than two times per calendar year.\(^{114}\)

A State Party must be notified of an inspection at least forty-eight hours prior to the arrival of the inspection team at the inspection site.\(^{115}\) Inspections may not last more than ninety-six hours, although extensions may be negotiated.\(^{116}\) The areas of the facility to be inspected are explicitly defined,\(^{117}\) as is the procedure that the inspection team must follow to request access to other parts of the site.\(^{118}\) The inspection team is permitted to take and analyze samples and to inspect records.\(^{119}\)

Inspections of Schedule 3 and "other relevant" facilities will verify the accuracy of declarations and the absence of Schedule 1 chemicals.\(^{120}\) Schedule 3 facilities will be randomly selected for inspection based on

---

\(^{108}\) Id. pt. VI, (23).

\(^{109}\) Id. pt. VII, (15).

\(^{110}\) Id. pt. VII, (16), (18). The following criteria will be considered: the toxicity of the scheduled chemicals, the quantity of the scheduled chemicals, the production capacity, and the capability of conversion for the purpose of initiating "production storage and filling" of toxic chemicals. Id. pt. VII, (18)(a)-(c).

\(^{111}\) Id. pt. VII, (16).

\(^{112}\) Id. pt. VII, (20).

\(^{113}\) Id. pt. VII, (21).

\(^{114}\) Id. pt. VII, (22).

\(^{115}\) Id. pt. VII, (29).

\(^{116}\) Id. pt. VII, (29).

\(^{117}\) See id. pt. VII, (28).

\(^{118}\) See id. pt. VII, (25).

\(^{119}\) Id. pt. VII, (26)-(27).

\(^{120}\) Id. pt. VIII, (17) (concerning Schedule 3 facilities) and pt. IX, (14) (concerning other relevant facilities).
equitable geographical distribution of inspections and on information relating to the chemicals, characteristics, and activities of the declared site. The State Party must be notified of the inspection at least 120 hours before the inspection team arrives at the site. The length of the inspection may not exceed twenty-four hours unless an extension is negotiated. As with Schedule 2 facilities, the inspection team may view records and take samples. The areas of the facility that may be inspected are expressly prescribed.

The routine inspection process for any declared site begins when the Technical Secretariat designates inspectors for the task. The Director General shall notify the inspected State Party before the planned arrival of the inspection team at the point of entry and must provide certain information concerning the inspection. Prior to each routine inspection, facility representatives must brief the inspectors regarding the nature and layout of the facility and any necessary safety and logistical considerations. Representatives of the inspected State Party may accompany the inspection team at all times and have the right to request and receive copies of the information and data gathered about the facility.

i. Document Searches and Photography

The inspection team is entitled to search documents and records and take photographs of, and samples from, the facility. The inspection team shall not operate any facility. If inspectors consider that, to fulfill their mandate, particular operations should be carried out in a facility, they shall request the designated representative of the in-

121. Id. pt. VIII, (14). "Other relevant" facilities will be selected by the same process, except that the Technical Secretariat may also consider proposals by Parties. Id. pt. IX, (11) (a)-(c). Except for challenge inspections, these types of facilities may not be inspected more than twice in a calendar year. Id. pt. IX, (12).
122. Id. pt. VIII, (25). For "other relevant" facilities, see pt. IX, (21).
123. Id. pt. VIII, (24). For "other relevant" facilities, see pt. IX, (20).
124. Id. pt. VIII, (21)-(22). For "other relevant" facilities, see pt. IX, (18)-(19).
125. See id. pt. VIII, (23). With regard to "other relevant" facilities, the inspection team may examine records only if the inspected signatory agrees that such access will aid the inspection. "Other relevant" facilities qualify for the "managed access" procedures discussed infra at notes 184-190 and accompanying text. Id. pt. IX, (17)-(18).
126. Id. pt. II, (1)-(9) (explaining the designation and acceptance of inspectors).
127. Id. pt. II, (31). "Notifications made by the Director-General shall include the following information: (a) the type of inspection; (b) the point of entry; (c) the date and estimated time of arrival at the point of entry; (d) the means of arrival at the point of entry; (e) the site to be inspected; (f) the names of inspectors and inspection assistants; (g) if appropriate, aircraft clearance for special flights." Id. pt. II, (32)(a)-(g).
128. Id. pt. II, (37).
129. Id. pt. II, (49)-(50).
130. Id. pt. II, (47)-(48). For a description of "Collection, handling and analysis of samples" under the CWC, see id. pt. II, (52)-(58).
spected facility to have them performed. The representative shall carry out the request to the extent possible.”

ii. Interviews of Personnel

To establish relevant facts, the inspectors may interview facility personnel in the presence of the representatives of the inspected State Party. If the inspected State Party deems questions to be irrelevant to the inspection, it has the right to object. If the inspection team chief believes, however, that the question is relevant, and s/he states its relevance, s/he must provide the question in writing to the inspected State Party for reply. In its report, the inspection team may note any refusal to permit interviews or to allow questions to be answered or explanations to be given.

iii. Post-Inspection Activities

Upon completion of the inspection, the inspection team must meet with representatives of the inspected State Party and the facility to share the preliminary written findings of the inspection. Within ten days, the inspection team must prepare a final report based on the inspection’s findings and submit it to the inspected State Party, which in turn may annex comments. The final report, with comments, must be submitted to the Director General of the Technical Secretariat within thirty days after the inspection.

b. Challenge Inspections

Challenge inspections are the most revolutionary aspect of the CWC. Challenge inspections are intended to clarify and resolve questions of CWC noncompliance and may be conducted anywhere a violation is suspected. Each State Party is authorized to request an on-site challenge inspection, conducted by an inspection team designated by the Director General, of any site within the territory of, or under the jurisdiction or control of, another State Party. Presumably, this may include private homes as well as government and commercial property.

---

131. Id. pr. II, (40).
132. Id. pr. II, (46).
133. Id. pr. II, (60).
134. Id. pr. II, (62)-(63). The report, which shall be kept confidential, must also contain information as to the manner in which the inspected State Party cooperated with the inspection team. Id. pr. II, (62).
135. CWC, supra note 4, art. IX, (8).
136. Id.
Challenge inspections are relatively unconstrained, so as to fill in gaps that might otherwise exist in the overall CWC verification scheme. A State Party requesting a challenge inspection must limit the request to the CWC's scope and provide all appropriate information that forms the basis for concern as to possible noncompliance. Each State Party must refrain from making unfounded requests; a challenge inspection may be performed only to verify facts related to noncompliance. The challenge inspection may be prevented from taking place only if three-quarters of the Executive Council deem the request frivolous (the concerns are minor irregularities or excessively technical), abusive (the concerns are artificial or intended to harass), or clearly beyond the scope of the CWC challenge inspection provisions.

The inspected State Party must permit the Technical Secretariat to conduct a challenge inspection. These inspections are not refusable. The State Party also must make every effort to demonstrate compliance, provide access to the requested site, and assist the inspection team throughout the inspection. A State Party may, however, take measures to protect sensitive installations and prevent disclosure of confidential information not related to the CWC.

The Director General must transmit notice of the inspection to the inspected State Party at least twelve hours prior to the arrival of the inspection team at the point of entry. The Director General must issue an inspection mandate, which states the inspection request in operational terms and governs the conduct of the challenge inspection. The inspection team must conduct the inspection in the least intrusive manner possible.

The site must be designated by the requesting State Party as precisely as possible by providing a site diagram that specifies the site's requested perimeter. The inspectors must arrive at the specified point of entry as soon as possible. The inspected State Party must transport the inspectors to the periphery of the proposed area of

---

137. Id. art. IX, (9).
139. CWC, supra note 4, art. IX, (10).
140. Id. art. IX, (11) (a)-(b).
141. Id. art. IX, (20).
142. Id. art. IX, (11)(c).
143. Id. art. IX, (15).
144. Id. art. IX, (18). The inspection request must, at a minimum, contain the following information: the State Party to be inspected, the point of entry, the location of the inspection site, the size and type of inspection site, the concern regarding possible noncompliance and the nature and circumstances of the possible noncompliance, and the name of the observer from the requesting State Party. Verification Annex, supra note 25, pt. X, (4)(a)-(e).
145. CWC, supra note 4, art. IX, (19).
inspection within twenty-four hours of their arrival at the point of entry if the site is a declared facility, or thirty-six hours if it is an undeclared facility.147 If requested, the inspected State Party may provide aerial access to the inspection site.148

i. Pre-inspection Activities

The inspected State Party must begin “securing the site” by compiling information about all vehicular activity at the site within twelve hours after the inspection team’s arrival.149 Upon arrival at the relevant perimeter, the inspection team must begin monitoring vehicular traffic activity.150 The team may also inspect vehicles exiting the site.151 Personnel and vehicles entering the site and personnel and personal passenger vehicles exiting the site are not subject to inspection. These procedures may continue for the duration of the inspection.152

The inspected State Party must provide the inspection team with a pre-inspection briefing, at which time the inspected State Party may indicate to the inspection team the areas, equipment, and documentation it considers sensitive and not related to the purpose of the inspection. Based on this briefing, the inspection team must prepare a plan specifying the activities to be carried out and the areas the inspection team wishes to inspect. This plan must be made available to the inspected State Party.153

ii. Inspection Activities

The inspected State Party must provide access within the requested perimeter within 108 hours after the arrival of the inspection team at the point of entry.154 The extent of access varies with the type of facility. For declared facilities with facility agreements, access must be unimpeded within the agreed boundaries. For declared facilities without facility agreements, access will be negotiated according to the CWC’s general inspection guidelines.155 Access must be granted to the

---

147. Id. pt. X, (13)-(15).
148. Id. pt. X, (40). Aerial access complements ground access to the inspection site and is not an alternative to it. KRUTZSCH & TRAPP, supra note 138, at 487.
149. Verification Annex, supra note 25, pt. X, (23). This information must be given to the inspection team and may include: traffic logs, photographs, and video recordings. Id. pt. X, (23)-(24).
150. Id. pt. X, (25).
151. Id. pt. X, (29). Such inspection will be conducted pursuant to the managed access procedures discussed below. See notes 184–190, infra, and accompanying text.
152. Id. pt. X, (30)-(31).
155. Id. pt. X, (51).
greatest degree possible, "taking into account any constitutional obligations [that the State Party] may have with regard to proprietary rights or searches and seizures." Those limitations may not be invoked to conceal evasion of CWC obligations nor to engage in prohibited activities; if invoked, the inspected State Party must make every reasonable effort to provide alternative means to clarify the possible noncompliance concern that generated the challenge inspection.

Although challenge inspections are relatively unconstrained, the inspection team may use only those methods necessary to provide sufficient relevant facts to clarify the noncompliance concerns; it cannot seek or document clearly unrelated information. It should conduct the inspection in the least intrusive manner possible, proceeding to more intrusive procedures only as it deems necessary. The inspection must not exceed eighty-four hours unless the inspected State Party agrees to an extension. Upon completion of the inspection, the inspection team and the observer must leave the inspected State Party's territory in the minimum time possible.

3. Provisions to Protect CBI

The CWC's procedures for CBI protection are more extensive than most domestic statutes dealing with the government's handling of confidential information. Many CWC provisions concern the identification and preservation of confidential information revealed by CWC verification activities, such as the submission of declarations, on-site monitoring, and on-site inspections at private and government facilities. The CWC's provisions are presented in detail here because they

---

156. Id. pt. X, (41).
157. Id. pt. X, (44).
158. Id. pt. X, (44)-(45).
159. Id. pt. X, (57)-(58).
160. It is important to note that the international chemical industry played an important role in the negotiation of the CWC. It was recognized early on that without the cooperation and approval of the very industry to be regulated, the CWC would be almost impossible to implement. The chemical industry's role in the negotiations was bolstered by the Government-Industry Conference Against Chemical Weapons, held in Canberra, Australia in 1989. At that conference, chemical trade associations representing 95% of the world's production capacity met with delegates and diplomats from 60 states; the groups agreed that industry would actively work with governments to ban chemical weapons. On the domestic front, the Chemical Manufacturers Association (CMA) advised United States negotiators as to the perspective of the United States chemical industry, particularly regarding verification procedures and the need to protect CBI. The CMA has supported a negotiated ban on chemical weapons since 1978. OTA REPORT, supra note 5, at 10. See also Kyle Olson, The U.S. Chemical Industry Can Live With a Chemical Weapons Convention, ARMS CONTROL TODAY, November 1989, at 21; Industry Urges Quick Implementation of U.N. Chemical Weapons Convention, supra note 15, at 79.
161. Under article VI of the CWC, all verification activities must avoid undue intrusion into a State Party's legitimate chemical activities. In addition, verification must proceed in accordance with the Confidentiality Annex. Confidentiality Annex, supra note 25, (10).
exemplify an important development that could be emulated in future agreements to prevent CBI disclosure as a consequence of disarmament.\textsuperscript{162}

\textbf{a. Responsibilities of the OPCW}

Most duties related to CBI protection fall to the OPCW. To protect confidential information, the OPCW will require only the minimum amount of information necessary to carry out its responsibilities.\textsuperscript{163} The Director General of the Technical Secretariat bears primary responsibility for protecting confidential information and establishing a stringent regime for its handling. Toward this end, it must develop agreements and regulations specifying what information States Parties must provide.\textsuperscript{164}

The CWC denotes information as confidential if: (1) the State Party so designates it; or (2) in the judgment of the Director General, the unauthorized disclosure of the information could cause damage to the State Party to which it refers (including private interests that the State Party represents) or to the mechanisms implementing the CWC.\textsuperscript{165} The level of sensitivity of confidential data is to be established based upon criteria categorized in a classification system that must be applied uniformly.\textsuperscript{166}

The Technical Secretariat will evaluate whether documents submitted by Parties contain confidential information.\textsuperscript{167} CWC-related information received by the OPCW generally will not be published or released.\textsuperscript{168} Confidential information will be securely stored at the OPCW or, in some cases, with the State Party.\textsuperscript{169} Information must be handled and stored in a manner that precludes the identification of the facility to which the information pertains.\textsuperscript{170}

\textsuperscript{162} These provisions are primarily contained in the Confidentiality Annex, supra note 25.
\textsuperscript{163} Id. (1)(a). Inspectors are also obligated to seek only information that is necessary to fulfill their mandate. Id. (8). Inspectors may not make records of information not related to CWC compliance. Id.
\textsuperscript{164} Id. (1)(2).
\textsuperscript{165} Id. (2)(a).
\textsuperscript{166} Id. (2)(d). This classification system will be developed by the Preparatory Commission.
\textsuperscript{167} Id. (2)(b). Such documents include: initial and annual reports and declarations, general reports on verification activities and other information provided in compliance with the CWC. Id. (2)(b)(i)-(iii).
\textsuperscript{168} Id. (2)(c). The exceptions are: (1) general information on the implementation of the CWC; (2) information released with the express consent of the state to which the information refers; and (3) confidential information released by the Organization pursuant to agreed procedures that ensure that release occurs only in strict conformity with the needs of the CWC. Id. (2)(c)(i)-(iii).
\textsuperscript{169} Id. (2)(e).
\textsuperscript{170} Id. (2)(f).
Access to, and handling of, confidential information by employees of the OPCW will be strictly controlled. Confidential information will be disseminated within the OPCW on a need-to-know basis. For each position in the Technical Secretariat, a formal description will specify the necessary access to confidential information.\(^\text{171}\) The Director General, inspectors, and other staff members must not disclose any confidential information that they have acquired in the course of their duties.\(^\text{172}\) Inspectors and staff members will be reminded about security considerations and possible penalties for improper disclosure.\(^\text{173}\)

b. Responsibilities of Parties

When a State Party receives information from the OPCW, including another State Party’s data, it must treat that information according to the level of confidentiality assigned by the OPCW.\(^\text{174}\) If requested, a State Party must furnish details as to its handling of that information.\(^\text{175}\) Special handling must be afforded to the data in accordance with the requesting State Party’s rights, CWC obligations, and the requirements of the Confidentiality Annex.\(^\text{176}\)

c. Protection of Confidential Information During Routine Inspections

Additional protections prevent the disclosure of confidential information during on-site verification activities. Before conducting inspections, the OPCW and the State Party must negotiate facility agreements for facilities subject to routine inspections. These agreements should include detailed and specific arrangements with regard to the following issues:

- areas of the facility to which the inspectors will be granted access;
- storage of confidential information on-site;
- scope of inspection in agreed areas;
- taking and analysis of samples;
- access to records; and
- use of instruments and continuous monitoring equipment.\(^\text{177}\)

\(^{171}\) Id. (6).
\(^{172}\) Id. (6)-(7). This obligation continues even after the end of their functions. Also, staff members must sign individual secrecy agreements with the Technical Secretariat covering the period of their employment and five years thereafter. Id. (9). The Preparatory Commission is currently drafting these agreements.
\(^{173}\) Id. (10).
\(^{174}\) CWC, supra note 4, art. VII, (6).
\(^{175}\) Confidentiality Annex, supra note 25, (4).
\(^{176}\) Id.
\(^{177}\) Id. (16).
States Parties may take measures they deem necessary to protect confidentiality so long as they fulfill their obligations to demonstrate compliance. During inspections (both routine and challenge), a State Party may indicate to the inspection team sensitive equipment, documentation, or areas that are not related to the inspection's purpose.178

Inspections are to be conducted in the least intrusive manner possible. The inspection team must consider the inspected State Party's proposals to ensure that sensitive equipment or information is protected.179 The proposals can be made at any time during the inspection. Moreover, the inspection team must fully respect any procedures designed to protect sensitive installations and to prevent the disclosure of confidential data.180 Once an inspection is completed, the report subsequently prepared must only contain facts relevant to the CWC. The report must be handled just as any other CWC confidential information. Where necessary, the information in the report will be processed into a less sensitive form prior to disclosure by the Technical Secretariat or the inspected State Party.181

d. Protection of Confidential Information During Challenge Inspections

Challenge inspections present special CBI concerns because they are particularly intrusive. Consequently, the inspection team may use only those methods necessary to provide sufficient relevant facts to clarify the concern about possible noncompliance, and must refrain from activities not relevant thereto. The inspection team may collect and document relevant facts, but may not seek or document information that is clearly irrelevant unless the inspected State Party expressly so requests. The inspection team may not retain any material collected and subsequently found to be irrelevant.182 The inspection team must conduct challenge inspections in the least intrusive manner possible, consistent with the effective and timely accomplishment of its mission, beginning with the least intrusive procedures it deems acceptable and proceeding to more intrusive procedures only as it deems necessary.183

Special “managed access” measures require the State Party and the inspection team to negotiate the extent of access to a facility in order to protect confidential information. The inspection team must consider any suggested modifications to the inspection plan or any other pro-

178. Id. (13).
179. Id. (14).
180. Id. (15).
181. Id. (17).
183. Id. pr. X, (45).
posals made by the inspected State Party to ensure that sensitive equipment, information, or areas not related to chemical weapons are protected.\textsuperscript{184} The inspected State Party and the inspection team shall negotiate: (1) the extent of access to any particular place(s) within the final and requested perimeters, as provided below; (2) the inspection team's particular activities, including sampling; (3) the performance of particular activities by the inspected State Party; and (4) provision of particular information by the inspected State Party.\textsuperscript{185}

The inspected State Party may take measures to protect sensitive installations and prevent disclosure of confidential information not related to chemical weapons, including: (1) removal of sensitive papers from office spaces; (2) shrouding sensitive displays, stores, and equipment; (3) shrouding sensitive equipment, such as computer or electronic systems; (4) logging off of computer systems and turning off of data-indicating devices; (5) restriction of sample analysis to presence or absence of chemicals listed in Schedules 1, 2, and 3, or appropriate degradation products; (6) using random selective access techniques whereby the inspectors may select a given percentage or number of buildings of their choice to inspect—the same principle can apply to the interior and content of sensitive buildings; and (7) in exceptional cases, giving only individual inspectors access to certain parts of the inspection site.\textsuperscript{186}

The inspected State Party must reasonably try to provide alternative means to clarify the possible noncompliance that generated the challenge inspection. Furthermore, it must reasonably try to demonstrate to the inspection team that any object, building, structure, container, or vehicle to which full access is not granted, or which is protected in the above manner, is not used for purposes related to the noncompliance concerns raised in the inspection request.\textsuperscript{187} This may be accomplished by means of, \textit{inter alia}: (1) partial removal of a shroud or environmental protection cover, at the discretion of the inspected State Party; (2) a visual inspection of the interior of an enclosed space from its entrance; or (3) other methods.

Using these managed access procedures, an inspected State Party is entitled to take measures necessary to protect national security, but may not invoke these limitations to conceal evasion of its obligations not to engage in activities prohibited under the CWC.\textsuperscript{188}

\textsuperscript{184} \textit{Id.} pt. X, (46).
\textsuperscript{185} \textit{Id.} pt. X, (47).
\textsuperscript{186} \textit{Id.} pt. X, (48).
\textsuperscript{187} \textit{Id.} pt. X, (49).
\textsuperscript{188} \textit{Id.} pt. X, (50).
As to scheduled chemical facilities declared under articles IV, V, and VI, the following managed access procedures apply: (1) for facilities with facility agreements, access and activities must be unimpeded within the agreed-upon boundaries; (2) for facilities without facility agreements, negotiation of access and activities shall be governed by the CWC's applicable general inspection guidelines; and (3) access beyond that granted for inspection of scheduled chemical facilities will be governed by the managed access procedures outlined above.

For facilities declared under article III, paragraph 1(d), if the inspected State Party, using managed access procedures, denies full access to areas or structures not related to chemical weapons, it shall make every reasonable effort to demonstrate to the inspection team that such areas or structures are not used for purposes related to possible CWC noncompliance.

e. Confidentiality of Samples

Sampling procedures may also protect some CBI. If sampling is conducted off-site during either routine or challenge inspections, the Director General is responsible for the security, integrity, preservation, and confidentiality of the samples. It must establish a stringent regime for their collection, handling, transport, and analysis. It must also certify the laboratories that perform analyses and oversee the standardization of procedures and equipment at those laboratories. The Technical Secretariat must account for samples, and unused samples must be returned to it.

f. Procedures in Case of a Breach of Confidentiality

The Director General must establish the procedures to be followed in the event of a breach or an alleged breach of confidentiality. If the Director General believes, with proper justification, that the obligation to protect confidential information has been violated, or if there has been an allegation to this effect, s/he may initiate an investigation. States Parties must cooperate and support the Director General

189. Id. pt. X, (51). This provision also applies to declared facilities under Articles IV and V. CWC, supra note 4, arts. IV–V.
191. Id. pt. II, (56).
192. Id. pt. II, (56)(a).
193. Id. pt. II, (56)(b)–(c).
194. Id. pt. II, (57).
196. Id. (19).
in any such investigation.\textsuperscript{197} Where a breach has been established, a State Party must take “appropriate action.”\textsuperscript{198}

If staff members breach confidentiality, the Director General must impose appropriate punishment or discipline.\textsuperscript{199} In serious cases, the Director General may waive the employee’s immunity from jurisdiction, but the OPCW cannot be held liable for any breach of confidentiality committed by its members.\textsuperscript{200} Where the OPCW and a State Party divulge confidential information, an ad hoc commission will settle the dispute.\textsuperscript{201}

The inability of a wronged State Party to seek effective redress from the OPCW raises serious concerns. The ability to sue the individual employee, if immunity is waived, will be of little benefit when the lost confidential information is worth millions of dollars. For all their innovation, the elaborate preventive measures in the CWC may be inadequate without an effective remedy for a wronged State Party.

\section*{III. CBI THEFT AND WRONGFUL DISCLOSURE}

\subsection*{A. Potential for CBI Loss}

Two aspects of arms control verification raise concerns about the loss of CBI. Both data reporting requirements and on-site inspections could lead to CBI loss as a result of industrial espionage or inadvertent release.

1. Loss Through Data Reporting Requirements

Under the CWC, and to a lesser extent under START,\textsuperscript{202} each State Party must submit declarations on the treaty-relevant activities of its domestic industries. These declarations will be based upon information—including CBI—provided by private industry. This process involves two steps. First, information must be gathered by a government agency from private firms. Second, that information must be sorted and declared to a foreign entity in a manner that complies with the international agreement. Inadequate CBI protection in the procedures

\begin{itemize}
\item \textsuperscript{197} Id. (21).
\item \textsuperscript{198} Id. (21). It is an open question as to what “appropriate action” might entail. The procedures to be followed in the event of a breach or an alleged breach of confidentiality, and presumably the resulting responsibilities of the States Parties, are to be developed by the Director General and approved by the Conference of State Parties. Id. (18).
\item \textsuperscript{199} Id. (18).
\item \textsuperscript{200} Id. (20), (22). State Parties must assist in the investigation of an alleged breach and assist in taking appropriate action if a breach is discovered. Id. (21).
\item \textsuperscript{201} Id. (22)--(23).
\item \textsuperscript{202} START does not contain any explicit data reporting requirements, but it is presumed that the government must gather treaty-related data from private industry.
\end{itemize}
of either the government or the international body that receives the information could cause leaks and the loss of valuable information.

The quantity of reported information is likely to be voluminous, complicating the task of protecting CBI. Information management requires a consistent format applicable to all Parties that is comprehensive, non-duplicative, and sufficiently timely so that treaty deadlines can be met. However, pressure to meet imminent and onerous deadlines may undermine efforts to maintain confidentiality.

2. Loss Through Inspections

On-site inspections pose different threats to CBI and are more susceptible to industrial espionage than are declaration requirements. For instance, during CWC inspections, CBI could be compromised or lost in many ways, including:

- manifests and container labels may disclose trade secrets about materials and the identity of key suppliers;
- panels may reveal the precise temperature and pressure conditions for specific production processes;
- analysis of residues taken from production line equipment may identify the unique reagents, catalysts, or other products made with that equipment;
- access to piping and instrumentation diagrams, combined with visual information, could reveal certain flow and process parameters; and
- audits of plant records, including customer lists and process documentation, could reveal CBI.

These concerns are underscored by the fact that inspectors with technical expertise will likely be recruited from private industry. Individuals who maintain strong ties to their home country, former employers, or a nationalized company (especially if they plan to return to those jobs) might be tempted to reveal trade secrets. An inspector could steal, stumble upon, or gain access to valuable CBI and disclose it, knowingly or not, to those who would misuse the information.²⁰³

B. Initiatives for Protecting CBI

Arms control inspections will differ from the types of inspections typically conducted by domestic authorities. As a result, owners of private facilities may not know how to prepare for them, particularly if they must reveal CBI to international inspectors. Advance prepara-

²⁰³. See generally OTA REPORT, supra note 5, at 50.
tion and planning could enable CBI owners to better understand arms control inspection procedures, possible data collection techniques, and the vulnerability of their own CBI, significantly minimizing the risk of CBI exposure. Of course, any techniques employed by private industry to protect CBI must comply with the inspection procedures of a particular arms control inspection. The following three suggestions could ease the transition to international arms control verification:

1. Preparation and Preventive Measures—The government and private facility owners should cooperate in initiatives to protect against theft or inadvertent disclosure of CBI.
2. Penalties for Wrongful Disclosure—Regulations should prohibit illicit disclosure and deter CBI theft by penalizing government personnel and, where possible, international inspectors for the knowing wrongful disclosure of CBI.
3. Remedies for Wrongful Disclosure—If CBI is wrongfully disclosed due to arms control activities, its owners should be given just compensation.

1. CBI Preparation and Protection Initiatives

While treaties contain measures to protect confidential information, as has been discussed regarding the CWC, it is probably unrealistic to assume that, by themselves, these measures sufficiently prevent improper disclosure. The United States government and facility owners should also pursue initiatives to protect CBI. Measures could include: (1) identifying and marking CBI in advance; (2) making preparations at the facility to be inspected; and (3) educating private industry about arms control inspections. The two principal goals of these measures are to limit the amount of CBI to which inspectors will have access and, where access to CBI is necessary, to ensure that inspectors and officials entrusted with CBI know that the information is CBI and is to be handled according to applicable protective measures.

204. See generally H.R. 4849, 103d Cong., 2d Sess. (1994) and S. 2221, 103d Cong., 2d Sess. (1994) (introduced by request in identical form in both Houses of Congress) [hereinafter President's Proposed CWC Implementing Legislation]. While none of the initiatives discussed in this subsection are included among its terms, this bill contains a number of provisions to integrate the CWC with domestic federal law. For example, it specifies that, "to the extent possible consistent with the obligations of the United States pursuant to the [CWC], no inspection . . . shall extend to—(A) financial data; (B) sales and marketing data (other than shipment data); (C) pricing data; (D) personnel data; (E) research data; (F) patent data; or (G) data maintained for compliance with environmental or occupational health and safety regulations." Id. § 401(e)(2). Furthermore, it presumes that optional facility agreements permitted by the CWC are to be concluded "unless the owner and the operator, occupant or agent in charge of the facility and the Technical Secretariat agree that such an agreement is not necessary." Id. § 401(0)(2). Such private persons are to "participate in the negotiation of all facility agreements" to the extent practicable. Id. § 401(0)(3).
To implement arms control CBI protection measures in the United States, the government will have to work closely with private industry and, in particular, any firm that will be regulated by a specific agreement. The initiatives designed to minimize the amount of CBI disclosed during arms control inspections and to protect any CBI that is divulged must ultimately be employed by private industry. However, all CBI protection measures should be taken under the careful guidance of the United States government.

a. Identification of CBI in Advance

A critical element of CBI protection is ensuring that the United States is made aware of all CBI that could be revealed at a particular facility. The facility owner should be given an opportunity to point out two types of CBI: (1) CBI that is irrelevant to the arms control agreement and should not, therefore, be revealed to arms control inspectors; and (2) CBI that could be relevant but should be entitled to protection from wrongful disclosure.

This process will likely require that the CBI owner consult with the government, which should develop formal guidance on identifying, marking, and submitting relevant information. To further these goals, the following initiatives could be considered:

- plant equipment and processes that are particularly sensitive and vulnerable to observation could be identified by companies and indicated to the government;
- processes and equipment could be examined to determine which aspects could be protected or shielded from view;205 or
- the government could specify the documents that must be shown to arms control inspectors.

A similar approach can be seen in federal statutes that require CBI disclosure. Several such statutes permit the owner to submit CBI separately or to mark that information as CBI. For example, under the Federal Insecticide, Fungicide, and Rodenticide Act (FIFRA), in submitting data to the Environmental Protection Agency (EPA), applicants may mark information that, in their opinion, consists of "trade secrets or commercial or financial information,"206 and submit it separately from other materials.207 Companies could develop internal procedures to ensure that CBI revealed during arms control inspections is

205. See OTA REPORT, supra note 5, at 50-52.
207. Id.
appropriately marked as CBI and to submit only CBI that is expressly required.

b. Plant Preparation

Private firms could take several steps in preparing a facility for an upcoming arms control inspection. To assist facility owners, the government could issue guidance on inspection procedures and inform them of acceptable methods of protecting CBI. So long as mandatory inspection procedures are observed and the aims of the treaty are not frustrated, facility owners could take the following steps:

- an inspection route within the facility could be developed to keep inspectors away from areas irrelevant to arms control verification;
- plant personnel could be trained to escort arms control inspectors;
- plant personnel could be trained as to what is likely to be inspected, how CBI should be protected in work areas, and how to respond to arms control inspection team questions without unnecessarily revealing CBI;
- shrouds, boxes, and screens could be installed around proprietary items, provided these measures do not interfere with the inspection's aims; and
- procedures could be developed to secure computers and sensitive documentation.208

To accomplish these plant preparation measures, the government could help industry to determine the most cost-effective means of protecting CBI. This determination will be a function of what is actually required by the arms control agreement in question and will prevent companies from needlessly employing costly methods to protect CBI.

c. Educational Programs to Assist Private Industry

Government programs could educate private businesses about what to expect from arms control activities. One possible initiative would be to develop and distribute a manual that provides guidance on the following issues: (1) a description of information that the government will treat as confidential; and (2) techniques to identify and mark CBI in a manner consistent with government guidelines (e.g., different marks for true trade secrets and other types of confidential or proprietary business information, etc.).

---
208. The government could assist in these efforts by providing material aid, such as temporarily providing facilities with shrouding materials. See OTA REPORT, infra note 5, at 51.
Other government initiatives could further educate private firms about means to protect CBI and thereby minimize concerns about CBI. These measures might include: (1) conducting trial or mock inspections at selected facilities,\textsuperscript{209} evaluating company methods for protecting CBI, and publishing findings; (2) encouraging communication between the government and inspected firms to verify CBI designations and consult on other issues; (3) performing vulnerability assessment programs (i.e., assessing the vulnerability of a facility and identifying areas in particular need of protection);\textsuperscript{210} or (4) sponsoring inspection preparation, training, and education seminars.

2. Prohibit CBI Revelation by United States Officials

CBI protection could be further enhanced if the government severely limited, or even prohibited, the public disclosure of CBI that has been collected during arms control activities. Removal from office and criminal penalties (fines and/or imprisonment) can effectively deter federal employees from wrongfully disclosing CBI.

The government could take procedural and administrative measures to minimize the risk of losing CBI gathered during arms control activities and to ensure its careful handling. First, government employees handling CBI should be of the highest integrity and should be screened before being employed. Second, such employees should be required to sign confidentiality agreements or otherwise pledge to maintain the confidentiality of designated information. Third, dissemination of CBI within and among government agencies should be limited to what is absolutely necessary to arms control or other law enforcement.\textsuperscript{211} Fourth, all CBI, including computerized information, should be stored in secure locations.

Many federal statutes already require private firms to disclose CBI to government agencies.\textsuperscript{212} To counter the risk of wrongful disclosure,

\textsuperscript{209} The United States, along with many other CWC signatories, has already participated in several National Trial Inspections (NTIs) to test procedures for routine and challenge inspections under the CWC. While NTIs are dedicated primarily to developing and refining verification techniques, they have also been useful in assessing the impact of CWC inspections on private industry. OTA REPORT, supra note 5, at 28 and sources cited therein.

\textsuperscript{210} See id. at 52–53.

\textsuperscript{211} The President's Proposed CWC Implementing Legislation, supra note 204, permits disclosure of information acquired by the United States under its terms only to: the Technical Secretariat; other States Parties to the Convention; Congressional committees and subcommittees; other agencies or departments for law enforcement purposes; or if the United States National Authority (which will be established to serve as the national focal point for CWC liaison, id. § 101) deems disclosure to be in the national interest. Id. § 302(a).

Congress has enacted prohibitions against CBI disclosure by federal officials. In addition, many of the statutes that compel disclosure of CBI also contain explicit penalties for officials who wrongfully reveal reported information. These statutes provide excellent models for trade secret protections that could be formulated for arms control activities.

The Trade Secrets Act (TSA)\textsuperscript{213} is a criminal statute that expressly forbids federal employees from disclosing trade secrets or other forms of confidential information unless authorized by law. Knowing disclosure by a federal employee is wrongful if the information is confidential in the sense that: 1) its disclosure is forbidden by official agency policy, agency regulation, or by law;\textsuperscript{214} or 2) its disclosure would cause substantial harm to the competitive position of the person from whom the information was obtained.\textsuperscript{215} Wrongful disclosure could subject the federal employee to a $1,000 fine, up to one year in prison, or both. The employee will also be removed from his/her federal position.\textsuperscript{216} The TSA prohibition against disclosure takes precedence over federal statutes with broad disclosure policies and bars disclosure even if the information was submitted under a government contract that allowed disclosure.\textsuperscript{217}

Other federal regulatory statutes take steps to protect trade secrets and punish wrongful CBI disclosure in either of two ways. First, some statutes simply incorporate the TSA and prohibit the release of any trade secret or confidential information that is not authorized by law.

Other statutes provide that the TSA does not apply to disclosures under the particular statute and, instead, enact stiffer penalties for wrongful disclosure. For example, under FIFRA, officers or employees of the United States frequently obtain possession of, or access to, information the disclosure of which is prohibited. If that officer or employee willfully and knowingly discloses this information to a person not entitled to receive it, s/he can be fined up to $10,000, be imprisoned for up to one year, or both. These penalties also apply to government contractors and their employees.\textsuperscript{218}


\textsuperscript{214} United States v. Wallington, 889 F.2d 573 (5th Cir. 1989).


\textsuperscript{217} Megapulse, Inc. v. Lewis, 672 E2d 959, 965 (D.C. Cir. 1982).

\textsuperscript{218} The penalties found in the Trade Secrets Act, discussed above, do not apply to wrongful
Extending these protections to arms control-generated information could be accomplished in several ways. First, Congress could enact a specific prohibition against the disclosure of CBI gathered during arms control activities with stiffer penalties than the TSA, thus creating an even greater deterrent. Second, government agencies authorized to handle CBI could implement a policy barring CBI disclosure, thus triggering the TSA. These proscriptions could be specifically directed against officials authorized to process arms control information or to participate in arms control inspections.

3. Recompense for Lost CBI

If the prohibitions against wrongful CBI disclosure work properly, there should be little need for judicial redress. No matter how comprehensive and well-administered the scheme for protecting trade secrets, however, CBI may be lost. Yet, neither START nor the CWC contains a mechanism for compensating the owners of CBI that is stolen or inadvertently disclosed due to verification activities. It would be unreasonable to rely exclusively on statutory prohibitions without allowing recovery of damages if CBI is, in fact, revealed.

This subsection discusses several possible avenues of redress in the context of CBI loss due to arms control activities. As will be demonstrated, serious hurdles face a claimant who alleges CBI loss due to the reporting or inspection requirements of arms control treaties. Without a damages remedy, a claimant could seek injunctive relief that could interfere with the operation of arms control treaties. Therefore, Congress should provide alternative remedies.


219. The President's Proposed CWC Implementing Legislation, supra note 204, criminalizes knowing and willful disclosure or provision of any CWC information contrary to its disclosure provisions by present or former officers or employees of the United States. Violation of this provision could result in a fine, imprisonment of up to five years, or both. Id. § 302(c).


221. The President's Proposed CWC Implementing Legislation, supra note 204, would prohibit court injunctions or other orders "that would limit the ability of the Technical Secretariat to conduct, or the United States National Authority or the lead agency to facilitate inspections as required or authorized by the [CWC]." Id. § 406(c). However, the bill includes no provision
along the lines suggested herein could encourage cooperation with arms control verification efforts by assuring CBI owners that they may seek compensation if they suffer losses.

a. Suits Against Other Parties to a Treaty

A suit against a foreign party or its inspectors who divulge CBI is not likely to be successful. A United States firm could sue a foreign government in United States federal courts for the actions of foreign civil servants that cause damages or loss of property. However, that party will enjoy sovereign immunity. A sovereign government cannot be sued unless it consents to suit or, in effect, waives its sovereign immunity. In addition, a private lawsuit against a party to an international agreement to which the United States is also a party would create a politically sensitive situation. Finally, a suit against a foreign government would be an incredibly complex and expensive endeavor. United States courts may not have jurisdiction over such a suit, and the plaintiff may be forced to bring suit in a foreign jurisdiction, under foreign law. Simply put, suits against other states are not a feasible means of recovery for lost CBI.

b. Suits Against Arms Control Organizations and Personnel

Because both START and the CWC grant inspection team members legal immunities during their entire stay within the inspected party’s territory, recovery from a member of the inspection team would also be unlikely. START inspectors and monitors enjoy the same immunities as diplomatic agents under article 31, paragraphs 1, 2, and 3 of the Vienna Convention on Diplomatic Relations. Immunity can be

---

223. See, e.g., Inspection Protocol, supra note 29, at art. II, para. 7.
224. Id. art. II, para. 7(e). Article 31, paragraphs 1, 2, and 3, of the Vienna Convention on Diplomatic Relations states:
   1. A diplomatic agent shall enjoy immunity from the criminal jurisdiction of the receiving State. He shall also enjoy immunity from its civil and administrative jurisdiction, except in the case of:
      (a) a real action relating to private immovable property situated in the territory of the receiving State, unless he holds it on behalf of the sending State for the purposes of the mission;
      (b) an action relating to succession in which the diplomatic agent is involved as executor, administrator, heir or legatee as a private person and not on behalf of the sending State;
waived by the inspecting State Party when immunity would impede justice, but any waiver must be express.\textsuperscript{225}

Similarly, under the CWC, the OPCW is accorded complete immunity concerning all acts performed in its official capacity necessary for the exercise of its functions.\textsuperscript{226} In short, the OPCW could probably only be liable to pay damages if it waived its immunity from jurisdiction.\textsuperscript{227} The CWC also grants legal immunity to OPCW personnel (e.g., members of the Technical Secretariat and all CWC inspection team members), including the absolute immunity from criminal and civil jurisdiction enjoyed by diplomats under article 31 of the Vienna Convention on Diplomatic Relations.\textsuperscript{228} However, OPCW personnel could be subject to civil or criminal jurisdiction if the OPCW waives an employee's immunity from jurisdiction.\textsuperscript{229}

It is important to note that the CWC limits the activities of inspection team members and provides that a State Party may have some form of redress if privileges and immunities are abused.\textsuperscript{230} Under the CWC's procedures to address an abuse of privileges and immunities, a State Party may (1) communicate all relevant information relating to abuses of privileges and immunities granted to the inspection team; and (2) consult with the Director General to determine whether there has been an abuse of privileges and immunities, and, if so, how to prevent a repetition of such an abuse.\textsuperscript{231}

\begin{itemize}
\item \textsuperscript{225} Inspection Protocol, \textit{supra} note 29, art. II, para. 7(e).
\item \textsuperscript{226} See CWC, \textit{supra} note 4, art. VIII, (48).
\item \textsuperscript{227} Under the CWC, the legal capacity, privileges and immunities of the OPCW will be defined in an agreement between the State Party and the OPCW. \textit{Id.} art. VIII, (50).
\item \textsuperscript{228} Verification Annex, \textit{supra} note 25, pt. II, (11)(e). \"[T]o exercise their functions effectively, inspectors and inspection assistants shall be accorded privileges and immunities ... for the entire period between arrival on and departure from the territory of the inspected State party [sic] or Host State, and thereafter with respect to acts previously performed in the exercise of their official functions.\" \textit{Id.} pt. II, (11). The President's Proposed CWC Implementing Legislation, \textit{supra} note 204, criminalizes knowing and willful disclosure or provision of any CWC information contrary to its disclosure provisions by employees of the Technical Secretariat. \textit{Id.} § 302(d).
\item \textsuperscript{229} The CWC allows the Director General of the OPCW to waive the immunity from jurisdiction of members of the inspection team if the Director General believes that immunity would impede the course of justice and that it can be waived without prejudice to the CWC's objectives. Any waiver of immunity must be express. Verification Annex, \textit{supra} note 25, pt. II, (14).
\item \textsuperscript{230} For example, inspectors cannot engage in any professional or commercial activity for personal profit during inspection duties. Inspection team members are also required to respect the laws and regulations of the inspected State Party, and they cannot interfere in the internal affairs of that State. See Verification Annex, \textit{supra} note 25, pt. II, (11)(d), (13).
\item \textsuperscript{231} \textit{Id.} pt. II, (13).
\end{itemize}
c. Suits Against the United States Government

i. For Torts Committed by United States Officials

If CBI is lost due to the wrongful conduct of a government official, a tort action may be available. The Federal Tort Claims Act (FTCA)\textsuperscript{232} makes the federal government liable for the negligence of its employees and establishes the circumstances under which the federal government has consented to suit against itself. "[The] United States shall be liable . . . to tort claims, in the same manner and to the same extent as a private individual under like circumstances."\textsuperscript{233} Yet the FTCA's waiver of sovereign immunity is limited by thirteen exceptions.\textsuperscript{234} If the government successfully invokes any of these exceptions, the plaintiff will not be able to recover.

Two exceptions are relevant to claims that could arise due to arms control activities. First, the United States is not liable for any claim based on the performance of a "discretionary function" by a federal official.\textsuperscript{235} This exception could prove problematic for those seeking recovery for damages caused by arms control activities because recent court decisions have broadly applied this exception to matters of national security.\textsuperscript{236}

Second, the United States will not be responsible for damages due to the commission of various intentional torts by federal employees if the commission was in good faith.\textsuperscript{237} The intentional torts listed by the exception include: "assault, battery, false imprisonment, false arrest, malicious prosecution, abuse of process, libel, slander, misrepresentation, deceit, or interference with contract rights."\textsuperscript{238} Therefore, CBI owners would only be able to recover if CBI was lost because inspectors acted in bad faith or without reasonable belief in the lawfulness of their activities.

\textsuperscript{232} Federal Tort Claims Act, 28 U.S.C. §§ 1346(b), 2671–2680 (1993). Before an FTCA suit can be filed, a claim must be presented to, and denied by, the responsible agency. \textit{Id.} § 2675. Agency heads are authorized to settle claims, but settlements greater than $25,000 must be approved by the Attorney General. \textit{Id.} § 2672.

\textsuperscript{233} \textit{Id.} § 2674.

\textsuperscript{234} \textit{Id.} § 2680.

\textsuperscript{235} \textit{Id.} § 2680(a). "At the core of the discretionary function is a recognition that regulatory decisions, such as promulgating rules and issuing licenses or permits, cannot give rise to a private cause of action without substantially interfering with the conduct of government." Barry Kellman, \textit{Judicial Abdication of Military Tort Accountability: But Who Is to Guard the Guards Themselves?}, 1989 Duke L.J. 1597, 1605.


\textsuperscript{237} 28 U.S.C. § 2680(b).

\textsuperscript{238} \textit{Id.}
actions. In addition, the exemption for torts arising from interference with contract rights could impede recovery for lost or stolen trade secrets.

Furthermore, recovery from the United States is a “complete bar” to a suit against the employee “whose act or omission gave rise to the claim.” In effect, an owner of lost CBI must elect whether to sue the United States under the FTCA or the individual government official in a Bivens action, discussed in Part III.B.3.d, infra.

ii. For Wrongs Committed by Foreign Officials or Inspectors

If the CBI loss is the result of the tortious conduct of a foreign official or inspector, a litigation alternative would be to sue the United States government. Chances of recovery against the federal government for disclosed CBI are remote under any circumstances, and even more obstacles appear in this context. A complication with holding the United States government liable for the improper acts of foreign officials or inspectors is proving they acted on behalf of the United States such that the government may be liable, even assuming sovereign immunity is waived. The judiciary has not ruled on the liability of the United States for torts committed by foreign officials pursuant to the verification of an international agreement.

Logic and fairness suggest that they should be deemed to be acting as government officials for purposes of assigning liability. The fundamental question is whether the inspection activities of the international organization manifest “state action” by the United States government, thereby triggering legal rights. “State action” may be defined as activity involving a sufficiently close nexus between the federal government and the challenged action so that it may fairly be treated as an endeavor of the United States. Accordingly, the federal government may be accountable when it so encourages the coercive power of another actor that the encroachment is deemed to be the responsibility of the government itself.

Domestic arms control inspections could be construed as actions of the United States because of the universally recognized principle of international law that holds that every state, as “a concomitant of sovereignty,” exercises jurisdiction over all persons, legal entities, and

---

objects within its physical boundaries.\textsuperscript{244} According to Chief Justice Marshall:

The jurisdiction of the nation, within its own territory, is necessarily exclusive and absolute. It is susceptible of no limitation not imposed by itself. Any restriction upon it, deriving validity from an external source, would imply a diminution of its sovereignty to the extent of its restriction, and an investment of the sovereignty, to the same extent, in that power, which could impose such restriction.\textsuperscript{245}

It is beyond dispute that arms control inspections encompass activity that has traditionally been a governmental function.\textsuperscript{246} The United States will be involved from the moment it issues the first inspector visa until it finishes reviewing the last inspection report.\textsuperscript{247}

d. Suits Against Federal Officials in Their Personal Capacities

Under \textit{Bivens v. Six Unknown Agents of the Federal Bureau of Narcotics}, a person can seek monetary damages against individual government agents for alleged violations of constitutional rights.\textsuperscript{248} As will be discussed below, wrongful disclosure of proprietary information by a government official could be a taking of private property in violation of the Fifth Amendment. Thus, a CBI owner whose constitutional property rights have been interfered with by a federal official could sue that federal official in his personal capacity.\textsuperscript{249}

\textsuperscript{245} Schooner Exchange v. McFadden, 11 U.S. (7 Cranch) 116 (1812).
\textsuperscript{246} According to a noted scholar:

The United States could agree to abolish existing armies and armaments, and to refrain from the raising of armies, and from the manufacture, possession or research and development of armaments in the future. It could agree to create a complex international organization to provide comprehensive inspection that would abolish the secrecy of governmental operations, require full reporting, and subject government installations, activities and files to unlimited surveillance, and its officials to international interrogation . . . .

That proposal might have given to an international authority power to regulate the activities not only of the Government of the United States but of manufacturers, scientists, laborers, and citizens generally. A body with such powers and functions would be exercising governmental authority within the United States, assuming functions of the President and Congress.\textsuperscript{247}

\textsuperscript{247} Louis Henkin, \textit{Foreign Affairs and the Constitution} 195–96 (1972) (emphasis added).

\textsuperscript{249} Although no case has been found in which a plaintiff recovered damages under the \textit{Bivens}
A Bivens suit must be distinguished from a suit under the FTCA. In a Bivens suit, the damages are paid by the government official personally responsible for the constitutional violation, whereas the federal government is responsible for paying the plaintiff who wins an FTCA case. Bivens suits are not available "when defendants show that Congress has provided an alternative remedy which it explicitly declared to be a substitute for recovery directly under the Constitution and viewed as equally effective."250 Therefore, if Congress were to create a compensation mechanism, a Bivens remedy would not be available for constitutional violations.251 A final consideration in bringing a Bivens action is that even though courts may recognize a claim, the federal official defendant can still raise immunity as a defense.252

e. Government-Administered Collective Insurance Fund

To avoid costly litigation, the government could establish a collective insurance fund. Firms potentially affected by arms control activities could pay into this fund based on such factors as their market share, the risk of loss posed to each firm, and the likelihood of a claim being made by that firm. The fund would then pay an amount of compensation for bona fide and reasonable claims for lost or stolen CBI. The United States could encourage the establishment of such a fund by: (1) paying a sum of money as a contribution to the fund; (2) assisting industry to set up the fund, including enacting laws to permit the existence of a private collective insurance fund; or (3) assisting in the adjudication of claims.

IV. CBI DISCLOSURE BY AGENCIES OF THE UNITED STATES

Arms control activities could cause the United States government to come into possession of CBI in several ways. For example, CBI might be disclosed in compliance with reporting requirements, revealed to officials prior to an inspection, or observed during an inspection and noted in the final inspection report. With large quantities of proprietary information coming into the hands of government officials, perhaps the gravest threat to CBI security is the possibility that information will be released legally. The vast majority of reported CBI presumably will not be classified, making it ripe for disclosure either

---

252. For a full discussion of the immunity of government officials (federal, state, and municipal) see Chemerinsky, supra note 241, § 8.6.
in response to a request from a private person or on the government's own initiative.

This problem should be distinguished from the problems discussed above concerning the release of CBI due to the malfeasance of either foreign inspectors or domestic officials. Those problems focused primarily on tortious conduct, either intentional or negligent. The solutions proposed focused primarily on steps that could be taken to reduce the risk of loss and, if necessary, on methods to compensate victims. Here, the problem is harmonizing the contradictory public interests of promoting openness while encouraging compliance with arms control reporting requirements.

This problem arises in two analogous contexts. First, reported CBI could be the subject of a request under the Freedom of Information Act (FOIA). Second, a federal official could disclose reported CBI in order to achieve some other governmental objective, raising an issue of whether the government's activity constitutes a taking entitling the owner to compensation under the Fifth Amendment. Whatever the legal justification for releasing information, regulations or agency policies should prohibit disclosure of CBI acquired as a consequence of arms control activities.

A. Freedom of Information Act (FOIA)

FOIA requires federal agencies to disclose their records to any person, including citizens, the media, academic researchers, and foreign governments and corporations, unless the records come under one of the Act's exceptions.

The information that must be disclosed includes information submitted to an agency as well as records created or compiled by the agency itself. The person requesting information is not required to give a reason for the request. The agency has the burden of proof for withholding the information.

If the agency refuses to disclose requested information, the requester may file a suit to force disclosure. FOIA specifically provides a private right of action to compel disclosure for individuals denied access to agency-held records. However, no corresponding right was created for submitters to prevent the release of information.

254. FOIA was intended to make available "to any member of the public . . . all of the executive branch records described in its requirements." H.R. REP. No. 1497, 89th Cong., 2d Sess. 1, reprinted in 1966 U.S.C.C.A.N. 2418.
255. 5 U.S.C. § 552(a)(4)(B) provides in part that "[o]n complaint, the district court . . . has jurisdiction to enjoin the agency from withholding agency records and to order the production of agency records improperly held from the complainant."
If an agency chooses to disclose information, that decision will be subject to judicial review under the Administrative Procedure Act. In this way, submitters of information can challenge an agency decision to disclose that information as an abuse of discretion by filing a "reverse FOIA" lawsuit to prevent the disclosure. In the few cases involving information related to national security or involving the types of information that have been discussed here, "reverse FOIA" suits have not generally been successful.

FOIA raises special CBI concerns. The overwhelming majority of FOIA requests for files containing trade secrets and CBI submitted by private firms are made by foreign and domestic businesses (either directly or through intermediaries such as attorneys). It is imperative, therefore, to ensure that CBI disclosed due to arms control activities is not subsequently released pursuant to a FOIA request.

In enacting FOIA, Congress balanced the confidentiality of information submitted to the government with the public's right of access to government information by enacting nine exemptions to its mandatory disclosure requirements. Three of FOIA's nine exemptions—under which a government agency may, at its discretion, refuse to disclose requested information—may be relevant to addressing concerns raised by arms control activities. Agencies are not compelled to withhold confidential information but merely are permitted to do so. Consequently, agencies have considerable authority to release confidential information regardless of its sensitivity or exempt status.

257. In Chrysler Corp. v. Brown, 441 U.S. 281, 291-92 (1979), the Supreme Court denied a private right of action for submitters to enjoin agency disclosure under FOIA or the Trade Secrets Act but preserved the availability of reverse-FOIA actions by recognizing an alternative theory under Section 10(a) of the APA.


261. In enacting FOIA, Congress acknowledged that mistrust concerning federal agencies' devotion and/or ability to maintain confidentiality could induce submitters to withhold information from agencies that is necessary for the accomplishment of their regulatory mission. See H.R. Rep. No. 1497, supra note 254. At least one commentator, however, has suggested that perceptions that industry has been victimized by FOIA are not based on an analysis of actual facts. See Mark Q. Connelly, Secrets and Smokescreens: A Legal and Economic Analysis of Governmental Disclosures of Business Data, 1981 Wis. L. Rev. 207.

Exemption 1 allows agencies to refuse to disclose information relevant to national defense or foreign policy if the information is properly classified as secret pursuant to criteria established by an executive order.\textsuperscript{263} In the absence of an applicable executive order, though, Exemption 1 will probably not prevent the public disclosure of arms control-related CBI.\textsuperscript{264} To address this situation, an executive order could be issued creating a presumption of damage to national security for disclosure of confidential information submitted pursuant to disclosure requirements of specified treaties.\textsuperscript{265}

Exemption 4 covers "trade secrets and commercial or financial information obtained from a person...[that are] privileged or confidential."\textsuperscript{266} If CBI gathered under arms control agreements falls within Exemption 4,\textsuperscript{267} the federal agency in possession of such CBI will have the discretion to refuse a FOIA request.\textsuperscript{268}

Under Exemption 3, agencies are not required to disclose information pertaining to "matters that are specifically exempted from disclosure by statute...provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld."\textsuperscript{269} No federal statute pertains directly to information disclosed pursuant to arms control verification activities.\textsuperscript{270} Enactment of a statute that ex-
plicitly forbids the disclosure of arms control-related CBI would exempt this information from disclosure.†271 Until that happens, however, Exemption 3 is not likely to meaningfully protect arms control-related CBI.

Several federal statutes expressly prohibit disclosure to the public of CBI that the government gathers in specific regulatory contexts. For instance, under FIFRA, the EPA cannot make public any information that, in the Administrator's judgment, contains or relates to either trade secrets or commercial or financial information.†272 Similar provisions can be found in other statutes, including the Toxic Substances Control Act (TSCA)†273 and the Clean Air Act (CAA).†274

Statutes prohibiting disclosure of CBI typically contain exemptions that permit the agency in possession of CBI to communicate that information to other federal agencies or officers or allow disclosure to protect public health and safety.†275 CBI may also be disclosed at a public hearing or in findings of fact by the government agencies, if necessary.†276 Information may also be disclosed whenever disclosure is necessary to comply with an obligation of the United States under a treaty or other international agreement.†277 Disclosure might also be permitted when it is relevant to investigations and proceedings conducted by federal and (occasionally) state and local agencies.†278 A final exemption found in many statutes allows federal agencies to disclose trade secret information to government contractors and their employees when such information is necessary for the satisfactory performance of a government contract.†279 If the disclosure of CBI is limited, some or all of the above exemptions will likely need to be included.†280

from FOIA disclosure only information "obtained from declarations or inspections" under the CWC. This section could be interpreted to require disclosure of information reported to the United States Department of Commerce pursuant to § 301(a), but not declared by the United States to the OPCW.

271. For an example of an agency regulation giving effect to this exemption see 10 C.F.R. § 2.790(a)(5) (1994) (Nuclear Regulatory Commission regulations under the Atomic Energy Act).
272. Any such information must have been obtained from a person making a submission under the Act and be "privileged or confidential." 7 U.S.C. § 136h(b) (1994).
275. Even when information must be disclosed pursuant to these exemptions, it must be treated as CBI and its dissemination strictly limited. For instance, under the Atomic Energy Act, CBI communicated to federal officials, government contractors and parties to official proceedings will only be disclosed subject to a protective order or protective agreement. 10 C.F.R. § 2.790(b)(5).
278. Id. § 830(c)(2)(B)(A)–(D).
280. As to how this is handled by the President's Proposed CWC Implementing Legislation, supra note 204, see supra note 211.
Furthermore, disagreements may arise between the facility owner and the government as to what types of information should be classified as CBI and be entitled to protection. The facility owner may mark information as CBI, but the agency responsible for arms control compliance may disagree and propose to reveal that information. A similar situation could arise where the government possesses information marked as CBI following an inspection (e.g., CBI contained in a final inspection report) and proposes to disclose that information. Existing statutes contain procedures for the settlement of these disputes that could collectively provide a model for arms control. Under FIFRA, for example, the EPA must notify the submitter, in writing, of its intent to release information that the submitter believes to be protected from disclosure. The EPA cannot release the information without the submitter's consent for thirty days, during which period the applicant may institute an action in federal district court for a declaratory judgment that the information is protected from disclosure.

Some statutes require the submitter to show that the information sought to be withheld from public disclosure is a trade secret. Under the Emergency Planning and Community Right-to-Know Act (EPCRA), for instance, information will not be treated as CBI unless the submitter can show that it merits protection. Satisfying these

281. Commenting on § 302(a), see supra note 270, of the President's Proposed CWC Implementing Legislation, supra note 204, the Administration noted that "this provision will allow the U.S. Government to protect all information or materials supplied by industry without requiring an inquiry into whether there are proprietary interests in such information or materials." Statement for the Record by Donald A. Mahley, Acting Assistant Director, Bureau of Multilateral Affairs, United States Arms Control and Disarmament Agency and Head of the United States Delegation to the CWC Preparatory Commission, before the House Foreign Affairs Committee on the Proposed Chemical Weapons Convention, August 3, 1994, at 5 (copy on file with authors).

282. 7 U.S.C. § 136h(c). Where disclosure is deemed necessary to avoid or lessen an "imminent and substantial risk of injury to the public health," special expedited procedures apply, accompanied by a right of the CBI owner to bring suit to enjoin the disclosure. Id. § 136h(d)(3). The President's Proposed CWC Implementing Legislation, supra note 204, permits disclosure of information that would otherwise be protected by the Act "if the United States National Authority determines that such disclosure is in the national interest," id. § 302(a)(4), but only following notice "where appropriate" to the information submitter followed by a 30-day waiting period. Id. § 302(b). There is no right on behalf of the submitter to file suit to prevent disclosure.

283. This showing would entail evidence as to all of the following factors:
1) the information has not been previously disclosed to another person (except federal, state and local officials, an employee of the submitter, or a person bound by a confidentiality agreement);
2) the submitter has taken reasonable steps to protect the confidentiality of the information and intends to continue to take such measures;
3) the information is not required to be disclosed or made available to the public under any federal, state or local law;
4) disclosure of the information is likely to cause substantial harm to the competitive position such person; and
5) the identity of the substance is not readily discoverable through reverse engineering.
42 U.S.C. § 11042(b).
requirements constitutes a prima facie showing that the information is indeed CBI, and the information will be treated as confidential until the agency administrator makes a contrary determination.\textsuperscript{284} This determination can be challenged by either the petitioner or the trade secret owner.\textsuperscript{285}

A dispute resolution system concerning arms control CBI could be formulated on similar principles, although implementing it without the benefit of legislation raises unique issues.\textsuperscript{286} One alternative would be to propose, by executive order, a method to designate CBI and resolve potential disputes. Another alternative, applicable to government contractors, would be to address these issues as part of the contracting process (discussed at Part IV.B.3 \textit{infra}).

Perhaps the best alternative would be the use of pre-submission confidentiality agreements (PSCAs). These agreements allow an agency to provide guarantees of confidentiality prior to submission so as to encourage willful and complete disclosure by submitters.\textsuperscript{287} Courts have been unwilling, however, to prevent later agency disclosure of such information.\textsuperscript{288}

Additional measures relating to public disclosure could include the following: (1) requiring a statement expressing the need for the information and the purposes it will serve in requests for disclosure of CBI by persons or organizations outside the government; (2) requiring the responsible government agency to maintain records of all persons to whom disclosure has been made; and (3) limiting or prohibiting disclosure of CBI to foreign or domestic competitors or intermediaries. These measures could limit the abuse of statutes such as FOIA by foreign and domestic businesses as an inexpensive means of acquiring valuable CBI.

\begin{enumerate}
\item \textsuperscript{284} The need for such a determination can arise in two respects: (1) where a person petitions for the disclosure of the information, or (2) upon the initiative of the agency administrator. In either case, the agency administrator will require the CBI owner to supplement the explanation with detailed information to support the claim. \textit{Id.} § 11042(d).
\item \textsuperscript{285} \textit{Id.} The Atomic Energy Act contains similar provisions. 10 C.F.R. § 2.790(b)(1)-(4) (1994).
\item \textsuperscript{286} No such provision is included in the President's Proposed CWC Implementing Legislation, \textit{infra} note 204.
\item \textsuperscript{287} \textit{See}, e.g., 26 C.F.R. § 601.702(b)(4)(ii) (1994) (authorizing submitters of information to the IRS to request confidential treatment of all or a portion of their submission); 12 C.F.R. § 261.17(a) (1994) (requiring submitters of information to the Federal Reserve Board of Governors be notified of requests for information designated by the submitter as confidential); 15 C.F.R. § 4.7(d) (1994) (requiring the Office of the Secretary, Commerce Division, to "carefully consider" objections of a submitter of confidential information before disclosure of such information).
\item \textsuperscript{288} In \textit{Petkus v. Staats}, 501 F.2d 887 (D.C. Cir. 1974), the Court of Appeals for the District of Columbia held that a pre-submission confidentiality agreement does not eliminate the discretionary nature of the FOIA exemptions.
\end{enumerate}
B. Takings Under the Fifth Amendment

If the government agency responsible for treaty compliance turns over CBI to a private party or to another government agency for a use that results in the CBI's release, then the CBI owner may claim the property was “taken.” The Fifth Amendment to the Constitution provides that property may not be taken without just compensation. In 1984, the Supreme Court held for the first time that trade secrets constitute property. Therefore, trade secrets are protected from disclosure or uncompensated use by the government under the “takings clause.”

1. Defining a Compensable Taking

If trade secrets are “taken” by the government, the owner is entitled to the fair market value of the loss. If the government reveals a trade secret originally obtained for a public purpose without the owner’s permission, the owner may sue under the Tucker Act to recover the value of the lost trade secret. The Tucker Act provides that “[t]he United States Court of Federal Claims shall have jurisdiction to render judgment upon any claim against the United States founded . . . upon . . . any Act of Congress or any regulation of an executive department . . . .” Thus, if CBI is disclosed during the course of arms control verification activities, the United States may be liable for the value of the lost property.

A “taking” may include direct government seizure of the property interest, but a “taking” can also include “governmental action short of

---

289. The President's Proposed CWC Implementing Legislation, supra note 204, would permit disclosure to federal agencies for law enforcement purposes. Id. § 302(a)(3).

290. The “takings clause” of the Fifth Amendment provides: “No person shall . . . be deprived of . . . property, without due process of law, nor shall private property be taken for public use without just compensation.” U.S. CONST. amend. V.

291. Ruckelshaus v. Monsanto, 467 U.S. 986 (1984). “This general perception of trade secrets as property is consistent with a notion of ‘property’ that extends beyond land and tangible goods and includes the products of an individual’s ‘labour and invention.’” Id. at 1002.

292. While this discussion considers whether the Fifth Amendment can be a remedy for government disclosure of CBI by operation of law, it is conceivable that the Fifth Amendment could also apply to the problem discussed earlier: wrongful release of the confidential information, see supra part III.B.3.

If the government's action could be characterized as purposely placing CBI at risk of loss in order to enhance national and international security, but the United States cannot be sued under the FTCA, then the same act might possibly constitute “inverse condemnation” under the Fifth Amendment. See generally A.W. Gans, Annotation, Damage to Private Property Caused by Negligence of Governmental Agents as “Takings,” “Damage,” or “Use” for Public Purposes, in Constitutional Sense, 2 A.L.R. 2d 677 (1948). At present, no case law indicates that the Fifth Amendment remedy would be available for tortious disclosure of CBI.

293. See Laurence H. Tribe, American Constitutional Law, § 9-3, at 592 (2d ed. 1988) (noting that takings by the government are compensable).

294. Monsanto, 467 U.S. at 1019.

acquisition of title . . . if its effects are so complete as to deprive the
owner of all or most of his interest in the subject matter." Yet, just
because the government requires firms to disclose trade secrets does
not mean that an unconstitutional taking has occurred. Mandatory
disclosure of CBI to the government that is rationally related to a
legitimate regulatory interest in exchange for a government benefit is
not a taking if the firm is aware of the conditions under which the
information is submitted and how it is to be used. The Supreme
Court has identified three factors that a court should consider to
determine if a compensable taking has occurred: (1) the character of
the governmental action; (2) its economic impact; and (3) its interfer-
ence with reasonable investment-backed expectations. The third fac-
tor is significant because the government will be liable for the disclo-
sure or unauthorized use of a trade secret only if the federal action
contains an explicit assurance of confidentiality. If the government
breaches that guarantee and destroys the competitive advantage of
exclusive control over the data, then a taking occurs.

2. Compensation for Losses

Because the government must compensate the owner of property
that it takes, a CBI owner could sue the United States for alleged
losses. Some federal statutes anticipate the government's need to take
private property in order to fulfill important federal interests. These
statutes: (1) ensure that just compensation is paid when the govern-
ment takes constitutionally protected property for public use; and
(2) grant persons the right to sue the government in the event of a
dispute. These statutes constitute a waiver of sovereign immunity and
permit suits against the agency within the limits defined by the
statute.

Several federal statutes can be consulted as examples. For instance,
the Atomic Energy Act authorizes the Nuclear Regulatory Commission
(NRC) to "take, requisition, condemn, or otherwise acquire" nuclear
material, or interests in such material. The Act also provides that
"[j]ust compensation shall be made for any right, property, or interest
in property taken, requisitioned, or condemned." To do so, the ABA
requires the NRC to determine the value of taken property and pay

296. United States v. General Motors Corp., 323 U.S. 373, 378 (1945); South Carolina v.
297. Monsanto, 467 U.S. at 1006–07.
298. Id. at 1005 (citing PruneYard Shopping Center v. Robins, 447 U.S. 74, 83 (1980)).
299. The President's Proposed CWC Implementing Legislation, supra note 204, does not
explicitly provide an assurance of confidentiality. Compare id. § 4(3) with id. § 302(a).
300. Monsanto, 467 U.S. at 1006–07, 1011–12.
302. Id.
just compensation. If the amount determined by the NRC is unsatis-
factory to the claimant, the NRC will pay that person 75% of that
amount. The claimant may then sue in the United States Court of
Federal Claims, or in any federal district court, for an additional sum
constituting just compensation.\footnote{Id. § 2221 (1993).}

Another statute, FIFRA, defines when the EPA can use information
submitted by one applicant in order to consider the data submitted by
another applicant.\footnote{7 U.S.C. § 136a(c)(1)(F) (1993).} If an applicant submits an application for the
registration of a pesticide (or an amendment to an existing registra-
tion), the EPA cannot use data submitted by another data submitter
without the written permission of the original data submitter.\footnote{Id. § 136a(c)(1)(F)(ii).} The
agency administrator can use this information, without the permission
of the original data submitter, if the new applicant has made an offer
to compensate the original data submitter for the use of the data.\footnote{Id. § 136a(c)(1)(F)(ii).} The
terms and amount of compensation can be agreed upon by the
original data submitter and the applicant. If the parties cannot reach an agreement, the terms
and conditions will be determined by means of binding arbitration before the Federal Mediation

The result of this procedure is that the government can use trade secret
information that is submitted so long as the owner of the secret is
compensated for such use.

The Chemical Diversion and Trafficking Act\footnote{Id. § 830 (c)(4).} is another law that
prohibits the disclosure of CBI. Under that Act, "[a]ny person who is
aggrieved by a disclosure of information in violation of this section
may bring a civil action against the violator for appropriate relief."\footnote{Lindsey v. United States, 214 Ct. Cl. 574, 577–79, aff'd, 566 F.2d 1190 (Ct. Cl. 1977).}

These types of statutes or regulations could be models for arms
control implementation. Because the extent of recovery would be defined
and limited by the provisions of the statute, Congress would be able
to curb potential liability of CBI loss. A statutory compensation scheme
could also avoid litigation, which could prove burdensome to the
courts as well as the parties concerned and may be a costly and
unnecessary distraction to the government agency responsible for han-
dling arms control functions.

If a dispute arises, and if the potential for CBI loss is not covered
by a government contract or a federal statute, the aggrieved party is
entitled to sue the government under the Tucker Act. Because the
Tucker Act is merely a jurisdictional statute, the courts can award
damages only if the right to relief is provided by another law.\footnote{Id. § 830.} A
Tucker Act remedy is available where federal regulations such as data disclosure or data consideration provisions effect an uncompensated taking of CBI or trade secrets, unless Congress statutorily withdraws the federal court's Tucker Act jurisdiction.\textsuperscript{310} Thus, unless Congress were to state explicitly in a federal statute that the Tucker Act will not apply to claims for uncompensated takings arising from arms control activities, federal courts would be able to hear such claims.\textsuperscript{311}

As an alternative to litigating claims of losses, Congress could develop a non-burdensome administrative claims procedure, such as a panel charged with hearing claims for damages resulting from arms control activities.\textsuperscript{312} This panel could determine and award the level of just compensation to be paid by the government to the injured person. Any such procedure must afford the claimant due process of law. At a minimum, the claimant should be required to prove that the claimed loss, such as the loss of a trade secret, was a direct result of treaty compliance.

3. Government Contracts

The government procurement process could address many CBI concerns where the CBI owner is also a government contractor.\textsuperscript{313} Federal contracting agencies could include clauses in their contracts that require contractors to disclose all arms control-relevant information, including CBI, and to waive any claim for CBI that is subsequently disclosed. One mechanism to implement this policy would be for the government to modify the contract of any contractor whose facility could be the subject of an arms control inspection.\textsuperscript{314} However, contractors may not be willing to waive their interest in arms control-related proprietary information.

A less drastic measure would be to draft contract language that promises contractors that their CBI will be given some modicum of confidentiality. The government could also promise to pay some form of damages for legitimate claims of lost CBI. Damages could be predictably handled in a liquidated damages clause or a requirement for arbitration if trade secrets are lost. If a dispute were to arise over a government contract referring to the loss of CBI resulting from arms

\textsuperscript{311} For an interesting discussion of this situation, see Allied-General Nuclear Services v. United States, 12 Cl. Ct. 372 (1987).
\textsuperscript{312} TANZMAN, HARMONIZING, supra note 95, at 67.
\textsuperscript{313} For a discussion of the issues raised by using the government procurement process to accomplish arms control objectives, see generally id. at 15–18.
\textsuperscript{314} Modifications could be either "bilateral" (agreed to by both Parties) or "unilateral"
control activities, the aggrieved contractor would be entitled to sue the United States under the Tucker Act.

A CBI-related contract clause could also identify, in advance, the location and characteristics of CBI not related to the purposes of arms control. In this way, the government will be able to tailor inspection procedures, subject to treaty obligations, in a manner that does not permit the inspection team access to a facility's CBI. The government would also be given an opportunity to agree to protect specific CBI, rather than a blanket assurance that all CBI will be protected. The burden would then be placed on the private firm to identify all CBI that it believes could be threatened. Any failure to identify threatened CBI would be the firm's responsibility because the government would have made no guarantee of confidentiality as to unidentified CBI.

V. CONCLUSIONS

The procedures likely to be applied to verify arms control treaties are sufficiently intrusive to pose a legitimate threat to CBI. CBI vulnerability is a legitimate concern because the objectives of arms control are better served if the property interests of private industry are secure. Arms control can be implemented in a manner that both avoids potential CBI loss and compensates CBI owners for wrongful use or disclosure.

Together, the United States and affected industries can minimize the risk posed to CBI. The key to avoiding problems is for the federal government to work closely with private firms whose CBI could be revealed. This should be part of a larger campaign to educate firms that might be subject to arms control activities about identifying and marking CBI, inspection procedures, and disclosure requirements so that there can be a cooperative effort to devise acceptable methods of protecting CBI. Furthermore, the United States should formulate official policies to regulate the handling of CBI that comes into the government's possession as a result of arms control reporting and inspections, including limiting, or even prohibiting, the further disclosure of CBI. Finally, the United States could make sure that stiff criminal penalties result from the knowing disclosure of CBI by federal officials.

Even if preventive measures are implemented, CBI could still be lost. To handle this situation in a predictable and efficient manner, the (imposed on the contractor). A bilateral modification would better preserve the government-contractor relationship and control costs. A unilateral modification, though more expedient, could strain that relationship and complicate cost control. If it becomes desirable to provide for a waiver of all arms control-related CBI claims in every government contract, rather than on a contract-by-contract basis, the Federal Acquisition Regulations could be amended to require a consent clause in all future government contracts.
government could pursue several avenues to compensate owners. An attractive option would be to develop a contract to govern specific situations or to establish an administrative claims panel to hear bona fide claims of CBI loss. Similar benefits could be achieved, on a broader scale, through federal legislation that sets out the circumstances under which the government will pay for CBI disclosure as a result of arms control verification and the compensation that will be paid for disclosed CBI. These options would avoid costly litigation and curb the potential liability of the United States by defining a remedy in advance. A final alternative to litigation would be establishment of a collective insurance fund, administered and partly funded by the United States, to allocate the risk of CBI loss.

In the absence of a pre-arranged compensation scheme (i.e., government contract, federal statute, or collective insurance fund), or if a compensation scheme proves inadequate, the government could be sued in the event of CBI loss. Lawsuits against the United States brought under the Tucker Act or the Federal Tort Claims Act could prove to be very costly and time consuming, and could result in unpredictable damages awards.

Disarmament presents new challenges to protecting CBI. Although United States law protects CBI in specific regulatory contexts, handles disputes between the federal government and private CBI owners, and compensates CBI owners, these laws were not developed with arms control in mind. Rather than rely on such complex and litigation-oriented mechanisms, it would make sense to develop regulatory remedies that harmonize the legitimate need to protect CBI with the need to verify arms control treaty compliance.